Security Requirements Document

Travel Agency Service

STS-Tool team

Feb 24, 2016

Table of Contents:

Introduction

This document describes the security requirements for the "Travel Agency Service"project. It provides a detailed description of: (I)social and organizational model, while capturing security requirements and automated analysis results; (II)secure business process models and procedural security policies, as well automated analysis and security policies enforcement;

Social and organizational models

This section provides a detailed description of the socio-technical security requirements models from different views (*Social*, *Information*, *Authorization*) and then presents the list of *security requirements* derived from them.

The *Social view* represents stakeholders as intentional and social entities, representing their goals and important information in terms of documents, together with their interactions with other actors to achieve these goals and to exchange information. Stakeholders express constraints over their interactions in terms of *security needs.* The *Information view* represents the informational content of stakeholders' documents, showing how information and documents are interconnected, as well as how they are composed respectively. The *Authorization view* represents which stakeholders own what information, and captures the flow of permissions or prohibitions from one stakeholder to another. The modelling of authorizations expresses other *security needs* related to the way information is to be manipulated.

The section ends with the list of *security requirements* for the system to be expressed in terms of *social commitments*, namely promises with contractual validity stakeholders make to one another. The security requirements are derived automatically once the modelling is done and the designer has captured the security needs expressed by stakeholders. Whenever a security need is expressed over an interaction from one stakeholder to the other, a commitment on the opposite direction is expected from the second stakeholder to satisfy the security need.

Social View

The social view shows the involved stakeholders, which are represented as *roles* and *agents*. Agents refer to actual participants (stakeholders) known when modelling the Travel Agency Service project, whereas roles are a generalisation (abstraction) of agents. To capture the connection between roles and agents, the *play* relation is used to express the fact that certain agents play certain roles.

Stakeholders have goals to achieve and they make use of different information to achieve these goals. They interact with one another mainly by *delegating goals* and *exchanging information*. Information is represented by means of documents, which actors manipulate to achieve their goals.

Social View Diagram

Figure 1 presents the graphical representation of the social view (a larger picture is shown in appendix A).

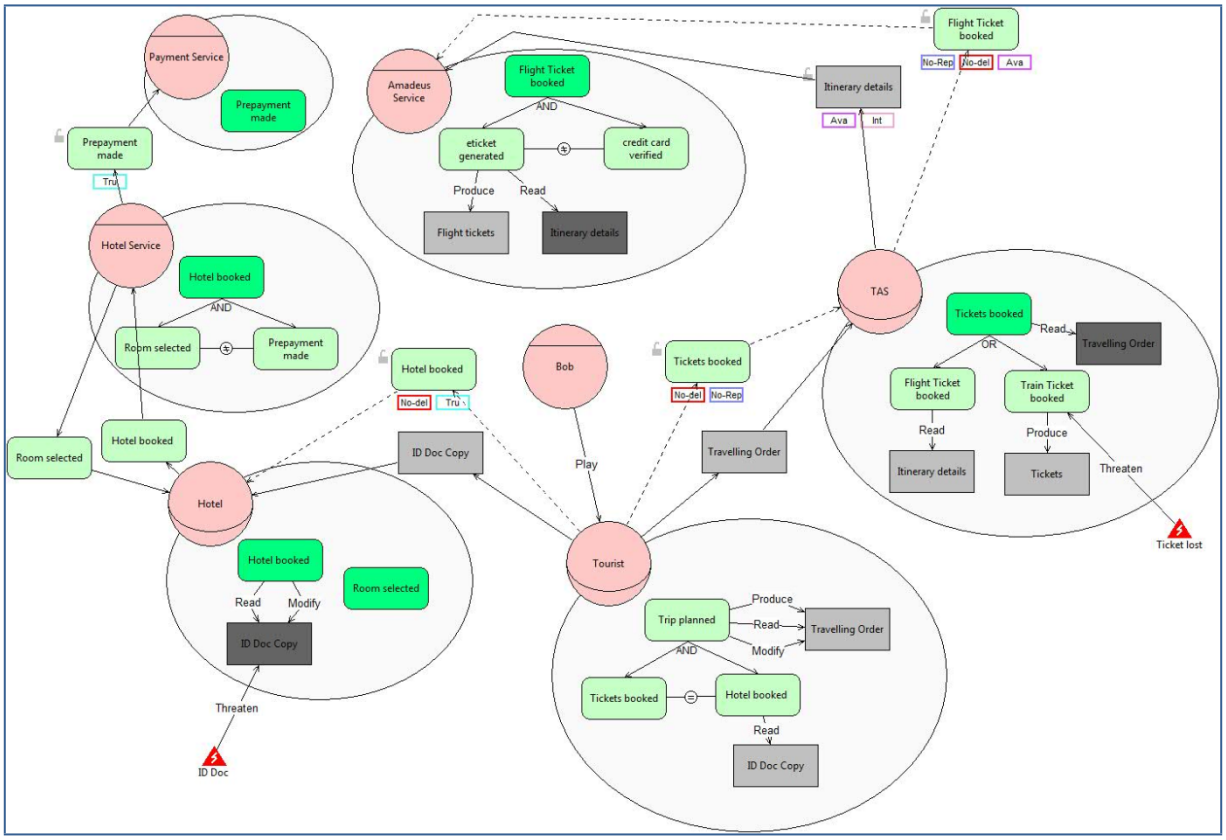

Figure 1 - Social View for the Travel Agency Service project

Stakeholders

This section describes the stakeholders identified in the Travel Agency Service project. Stakeholders are represented as roles or agents.

In particular, identified roles are: *Hotel*, *Tourist* and *TAS* (Figure 1), while identified agents are: *Bob*, *Hotel Service*, *Payment Service* and *Amadeus Service* (Figure 1). Table 1 and Table 2 summarise the stakeholders.

Role	Description	Mission	Purpose
Hotel			
Tourist			
TAS			

Table 1 - Roles in the Travel Agency Service project.

Agent	Description	Abilities	Important Features	Certifications Accreditations	Type Of Organisation
Bob					
Hotel Service					
Payment Service					
Amadeus Service					

Table 2 - Agents in the Travel Agency Service project

Agents and roles are related by means of *play* relations, as reported on Table 3

Agent	Role
Bob	Tourist

Table 3 - Agent/Role relations in the Travel Agency Service project

Stakeholders' documents

Stakeholders have documents they possess or exchange with others to achieve their goals. Documents are represented within the rationale of the role/agent (Figure 1).

In the Travel Agency Service project (Figure 1) we have:

- **Hotel** has document *ID Doc Copy* provided by *Tourist*.
- **Tourist** has documents *Travelling Order* and *ID Doc Copy*.
- **TAS** has documents *Itinerary details* and *Tickets*. Moreover it has document *Travelling Order* provided by *Tourist*.

- **Amadeus Service** has document *Flight tickets*. Moreover it has document *Itinerary details* provided by *TAS*.

Table 4 summarises stakeholders' *documents* for the Travel Agency Service project.

Agent/Role	Document	Description
Hotel	ID Doc Copy	
Tourist	Travelling Order	
	ID Doc Copy	
TAS	Travelling Order	
	Itinerary details	
	Tickets	
Amadeus Service	Itinerary details	
	Flight tickets	

Table 4 - Stakeholders' documents in the Travel Agency Service project

Stakeholders' documents and goals

Stakeholders' documents are linked to their goals: they read (make) documents to achieve their goals, they modify documents while achieving their goals, and they may produce documents from achieving their goals.

In the Travel Agency Service project (Figure 1) stakeholders' documents and goals are related as follows:

- **Hotel** *reads*, *modify* document *ID Doc Copy* to achieve goal *Hotel booked* .
- **Tourist** *reads* document *ID Doc Copy* to achieve goal *Hotel booked* and *reads*, *modify*and *produce* document *Travelling Order* to achieve goal *Trip planned*.
- **TAS** *reads* document *Travelling Order* to achieve goal *Tickets booked*, *reads* document *Itinerary details* to achieve goal *Flight Ticket booked* and *produces* document *Tickets* to achieve goal *Train Ticket booked*.
- **Amadeus Service** *reads* document *Itinerary details* and *produces* document *Flight tickets* to achieve goal *eticket generated*.

Table 5 summarises goal-document relations for all stakeholders in the Travel Agency Service project.

Agent/Role	Goal	Document	Relation
Hotel	Hotel booked	ID Doc Copy	read, Modify
Tourist	Hotel booked	ID Doc Copy	read
	Trip planned	Travelling Order	read, Modify, Produce
TAS	Tickets booked	Travelling Order	read
	Flight Ticket booked	Itinerary details	read
	Train Ticket booked	Tickets	Produce
Amadeus Service	eticket generated	Itinerary details	read

	Flight tickets	Produce

Table 5 - Relation of stakeholders' documents to their goals

Goal Refinement

Stakeholders have goals to achieve. Goals are represented within the rationale (round compartment attached to the role/agent, see Figure 1) of the role/agent representing the stakeholder. They achieve their goals by further refining them into finer-grained goals (subgoals) by means of AND/OR-decompositions. AND-decompositions structurally refine a goal into multiple subgoals (all AND subgoals need to be achieved for the goal to be achieved), while OR-decompositions represent alternative ways for achieving a goal (at least one of the subgoals in the OR-decomposition needs to be achieved for the goal to be achieved).

In the Travel Agency Service project (Figure 1) we have:

- **Hotel** has to achieve goal *Hotel booked* and goal *Room selected*.
- **Tourist** has to achieve goal *Trip planned*. To achieve *Trip planned*, Tourist should achieve goal *Tickets booked* and goal *Hotel booked*
- **TAS** has to achieve goal *Tickets booked*. To achieve *Tickets booked*, TAS should achieve either goal *Flight Ticket booked* or goal *Train Ticket booked*
- **Hotel Service** has to achieve goal *Hotel booked* . To achieve *Hotel booked* , Hotel Service should achieve goal *Room selected* and goal *Prepayment made*
- **Payment Service** has to achieve goal *Prepayment made*.
- **Amadeus Service** has to achieve goal *Flight Ticket booked*. To achieve *Flight Ticket booked*, Amadeus Service should achieve goal *eticket generated* and goal *credit card verified*

Table 6 summarises the goals of each agent/role in the Travel Agency Service project and how they are decomposed, when applicable.

Agent/Role	Goal	Dec. Type	Subgoals
Hotel	Hotel booked	-	
	Room selected	-	
Tourist	Trip planned	AND	Tickets booked
			Hotel booked
TAS	Tickets booked	OR	Flight Ticket booked
			Train Ticket booked
Hotel Service	Hotel booked	AND	Room selected
			Prepayment made
Payment Service	Prepayment made	-	
Amadeus Service	Flight Ticket booked	AND	eticket generated
			credit card verified

Table 6 - Goal Decompositions

Goal Contributions

Goals can contribute one to another. A contribution identifies the impact the fulfilment of one goal has on the fulfilment of another goal. This impact can be either positive or negative, and is represented with "++" and "--" respectively. Positive contribution means that the achievement of a goal also achieves the other goal. Negative contribution means that the achievement of a goal inhibits the achievement of another goal.

In the Travel Agency Service project there are no contribution relations taking place for the given agents/roles.

Stakeholders Interactions

This section describes stakeholders' interactions, providing insights on whom they interact with to fulfil their desired objectives, as well as which are the stakeholders that rely on them to fulfil their respective goals. This kind of interaction is carried out by means of *goal delegations*.

To achieve their goals stakeholders might need specific information. If they do not possess this information, they may ask other stakeholders to provide them documents. *Document transmission* is used to capture this interaction.

Goal Delegations

Stakeholders interact with others to achieve some of their goals by means of goal delegations. Goal delegations are graphically represented as a relation that starts from a delegator actor to a delegatee actor (following the direction of the arrow), having a rounded corner rectangle representing the goal being delegated. Security needs are graphically specified as labels that appear below the delegated goal (Figure 1).

The following description enlists all the delegations from one role/agent to the others. When applicable, security needs expressed over the delegations are enumerated.

In the Travel Agency Service project (Figure 1), we have the following goal delegations:

- **Hotel** delegates goal *Hotel booked* to **Hotel Service**.
- **Tourist** delegates goal *Tickets booked* to **TAS**.

  The following security needs apply to this delegation:

  No-Delegation and Non Repudiation: acceptance.
- **Tourist** delegates goal *Hotel booked* to **Hotel**.

  The following security needs apply to this delegation:

  No-Delegation and Trustworthiness.
- **TAS** delegates goal *Flight Ticket booked* to **Amadeus Service**.

  The following security needs apply to this delegation:

  Non Repudiation: acceptance, No-Delegation and Availability: 90.
- **Hotel Service** delegates goal *Prepayment made* to **Payment Service**.

  The following security needs apply to this delegation:

  Trustworthiness.

- **Hotel Service** delegates goal *Room selected* to **Hotel**.

Table 7 summarises *goal delegations*, together with the eventual *security needs* when applicable, and eventual description respectively.

Delegator	Goal	Delegatee	Security Needs	Delegation Description
Hotel	Hotel booked	Hotel Service		
Tourist	Tickets booked	TAS	**No-Delegation** **Non Repudiation**: *acceptance*	
	Hotel booked	Hotel	**No-Delegation** **Trustworthiness**	
TAS	Flight Ticket booked	Amadeus Service	**Non Repudiation**: *acceptance* **No-Delegation** **Availability**: *90*	
Hotel Service	Prepayment made	Payment Service	**Trustworthiness**	
	Room selected	Hotel		

Table 7 - Goal Delegations and Security Needs

Document Transmission

Stakeholders exchange information by means of documents with other stakeholders. The following description enlists all the transmission from one role/agent representing the stakeholder, to other roles/agents. *Document transmission* is represented as an arrow from the transmitter to the receiver, with a rectangle representing the document. The security needs expressed over the transmission are described, if applicable. Security needs are specified with the help of labels that appear below the document being transmitted.

In the Travel Agency Service project (Figure 1), we have the following *document transmissions*:

- **Tourist** transmit document *Travelling Order* to **TAS**.
- **Tourist** transmit document *ID Doc Copy* to **Hotel**.
- **TAS** transmit document *Itinerary details* to **Amadeus Service**.

  The following security needs apply to this transmission:

  Availability: 90 and Integrity: receiver.

Table 8 summarises the *document transmissions* for the Travel Agency Service project.

Transmitter	Document	Recivier	Security Needs	Transmission Descr.
Tourist	Travelling Order	TAS		
	ID Doc Copy	Hotel		
TAS	Itinerary details	Amadeus Service	**Availability**: *90* **Integrity**: *receiver*	

Table 8 - Document Transmissions and Security Needs

Organisational Constraints

Apart from the security needs actors specify over their interactions, there are others, which are dictated either by the organisation, business rules and regulations, or law. In this section we enlist these constraints, together with the security requirements derived from them. Currently, the language supports these organisational constraints: *Separation of Duties (SoD)* and *Binding of Duties (BoD)*. Graphically we represent these constraints using a similar notation to that used in workflows, as a circle with the *unequal* sign within and as a circle with the *equals* sign within, respectively. The relations are symmetric, and as such they do not have any arrows pointed to the concepts they relate (being these roles or goals).

In the Travel Agency Service project (Figure 1) the following organisational constraints have been specified:

- **Room selected** is incompatible with **Prepayment made**, given that *SoD* constraint is specified between these goals.
- **eticket generated** is incompatible with **credit card verified**, given that *SoD* constraint is specified between these goals.
- **credit card verified** is incompatible with **eticket generated**, given that *SoD* constraint is specified between these goals.
- **Prepayment made** is incompatible with **Room selected**, given that *SoD* constraint is specified between these goals.
- **Hotel booked** should be combined with **Tickets booked**, given that *BoD* constraint is specified between these goals.
- **Tickets booked** should be combined with **Hotel booked** , given that *BoD* constraint is specified between these goals.

Table 9 summarises the organisational constraints for the Travel Agency Service project.

Organisational Constraint	Role/Goal	Role/Goal	Description
SoD (Goal - Goal)	Room selected	Prepayment made	
	eticket generated	credit card verified	
	credit card verified	eticket generated	
	Prepayment made	Room selected	
BoD (Goal - Goal)	Hotel booked	Tickets booked	
	Tickets booked	Hotel booked	

Table 9 - Organisational Constraints

Events

Table 10 represents all the events modeled in the project Travel Agency Service together with the set of elements each event threatens. Additionally, for each reported event a textual description is provided.

Event name	Threatened elements	Description
ID Doc stolen	DocumentReference: ID Doc Copy	
Ticket lost	Goal: Train Ticket booked	

Table 10 - Events

Information View

The information view gives a structured representation of the information and documents in the Travel Agency Service project. It shows what is the informational content of the documents represented in the social view. Information is represented by one or more documents (*tangible by*), and the same document can make tangible multiple information entities. Moreover, the information view considers composite documents (information) capturing these by means of *part of* relations.

Information View Diagram

Figure 2 presents the graphical representation of the information view (a larger picture is shown in appendix A).

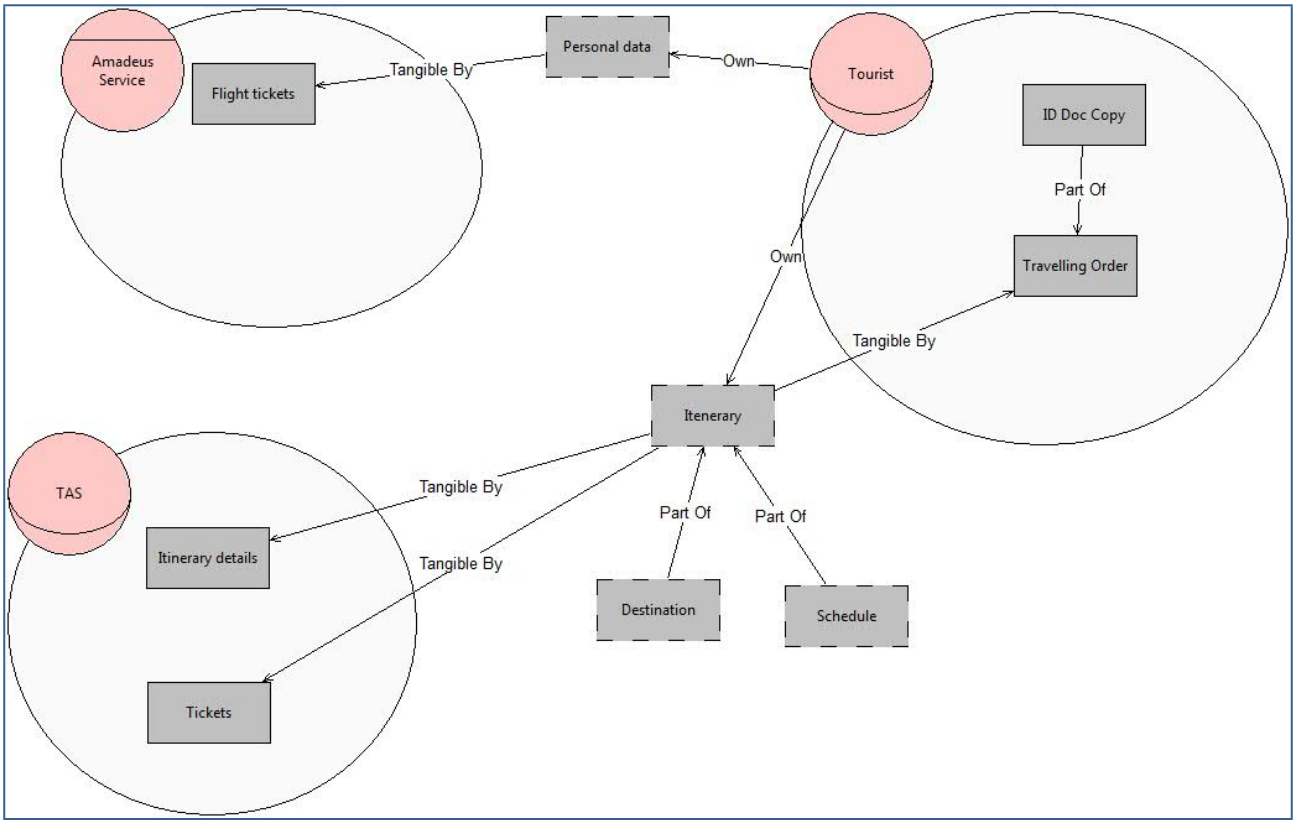

Figure 2 - Information View for the Travel Agency Service project

Modelling Ownership

The information view represents also who are the *owners* of the information that is being manipulated through the documents that represent them in the social view.

The owners for the different information in the Travel Agency Service project are summarised in Table 11.

Agent/Role	Information	Description
Tourist	Personal data	
	Itenerary	

Table 11 - Information owners

Representation of Information

Information is represented (*made tangible by*) by documents, which stakeholders have and exchange.

The documents stakeholders in the Travel Agency Service project (Figure 2) have and exchange with one another contain the information as summarised in Table 12:

Information	Document	Description
Itenerary	Itinerary details	
	Tickets	
	Travelling Order	
Personal data	Flight tickets	

Table 12 - Representation of Information through Documents

Structure of Information and Documents

Documents (information) are composed of other documents (information). Composition of documents (information) is captured through *part of* relations. This gives us an idea of how information and/or documents in the Travel Agency Service project are structured.

Table 13 and Table 14 summarises the information and documents in the Travel Agency Service project (Figure 2), showing how they are composed and describing the composition.

Information	Composition	Description
Itenerary	Destination	
	Schedule	

Table 13 - Information composition

Document	Composition	Description
Travelling Order	ID Doc Copy	

Table 14 - Documents composition

Authorization View

The authorization view shows the permissions or prohibitions flow from a stakeholder to another, that is, the authorizations stakeholders grant or deny to others about information, specifying the operations the others can and must perform over the information. Apart from granting authority on performing operations, a higher authority can be granted, that of further authorising other actors (i.e. authorization transferability)

Authorizations start from the information owner. Therefore, in the authorization view, ownership is preserved and inherited from the information view.

Authorization View Diagram

Figure 3 presents the graphical representation of the Authorization view (a larger picture is rappresented in appendix A).

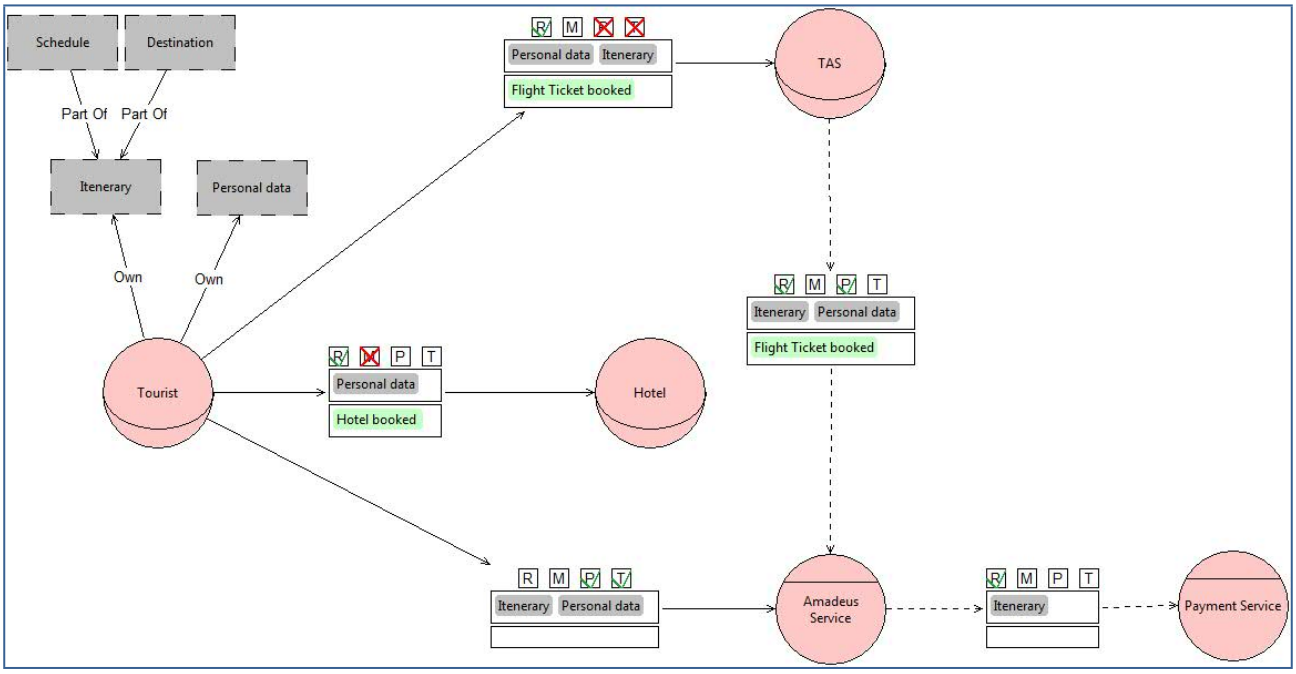

Figure 3 - Authorization View for the Travel Agency Service project

Authorization Flow

In this section are described for each role/agent, the authorizations it passes to others and what authorizations it receives from other roles/agents.In the Travel Agency Service project (Figure 3) the authorizations for each role/agent are:

- *Role* **Hotel**:
  - **Hotel** is authorised by *Hotel* to *read* and prohibited to *modify* information *Personal data*, in the scope of goal *Hotel booked* , *having* the right to further authorising other actors.
- *Role* **Tourist**:
  - **Tourist** authorises *TAS* to *read* and prohibits to *produce* and *transmit* information *Personal data* and *Itenerary*, in the scope of goal *Flight Ticket booked*, *passing* the right to further authorising other actors, and authorises *Amadeus Service* to *produce* and *transmit* information *Itenerary* and *Personal data*, *passing* the right to further authorising other actors, and authorises *Hotel* to *read* and prohibits to *modify* information *Personal data*, in the scope of goal *Hotel booked* , *passing* the right to further authorising other actors.
- *Role* **TAS**:
  - **TAS** authorises *Amadeus Service* to *read* and *produce* information *Itenerary* and *Personal data*, in the scope of goal *Flight Ticket booked*, *passing* the right to further authorising other actors.
  - **TAS** is authorised by *TAS* to *read* and prohibited to *produce* and *transmit* information *Personal data* and *Itenerary*, in the scope of goal *Flight Ticket booked*, *having* the right to further authorising other actors.
- *Agent* **Payment Service**:
  - **Payment Service** is authorised by *Payment Service* to *read* information *Itenerary*, *having* the right to further authorising other actors.
- *Agent* **Amadeus Service**:
  - **Amadeus Service** authorises *Payment Service* to *read* information *Itenerary*, *passing* the right to further authorising other actors.
  - **Amadeus Service** is authorised by *Amadeus Service* to *read* and *produce* information *Itenerary* and *Personal data*, in the scope of goal *Flight Ticket booked*, *having* the right to further authorising other actors, and is authorised by *Amadeus Service* to *produce* and *transmit* information *Itenerary* and *Personal data*, *having* the right to further authorising other actors.

Security Requirements

This section provides the list of security requirements derived for the Travel Agency Service project.

The list of security requirements shows the roles/agents that are *responsible* to satisfy them, so that stakeholders know what they have to bring about in order to satisfy the corresponding security needs. Security requirements also include the authorizations granted by stakeholders to other stakeholders.

Security needs are expressed mainly over goal delegations, document provisions and authorizations. Therefore, the list of security requirements is derived from every type of security need. Moreover, the organisational constraints specify further *needs* over roles and goal, leading to the generation of other security requirements.

Finally, the *requester* actors are represented to capture the actors requiring certain security needs to be brought about.

The security requirements for the Travel Agency Service project (Table 15) are:

- **Tourist** requires *TAS no-delegation* on goal *Tickets booked* and *non-repudiation-of-acceptance* of the delegation of goal *Tickets booked*, when delegating *Tickets booked* to *TAS*; while it requires *Hotel no-delegation* on goal *Hotel booked* and *trustworthiness*, when delegating *Hotel booked* to *Hotel*.
- **Tourist** requires *TAS* the *non-production* and *non-disclosure* of information *Personal data* and *Itenerary*, and *need-to-know* of these pieces of informations for the goal *Flight Ticket booked*, when authorising *TAS* to *read Personal data* and *Itenerary* in the scope of goal *Flight Ticket booked*; while it requires *Hotel* the *non-modification* of information *Personal data*, and *need-to-know* of these pieces of information for the goal *Hotel booked* , when authorising *Hotel* to *read Personal data* in the scope of goal *Hotel booked* .
- **TAS** requires *Amadeus Service no-delegation* on goal *Flight Ticket booked*, *non-repudiation-of-acceptance* of the delegation of goal *Flight Ticket booked* and an *availability* level of 90%, when delegating *Flight Ticket booked* to *Amadeus Service*.
- **TAS** requires *Amadeus Service* an *availability* level of 90% and a *receiver-integrity* , when transmitting *Itinerary details* to *Amadeus Service*.
- **Hotel Service** requires *Payment Service trustworthiness*, when delegating *Prepayment made* to *Payment Service*.
- *Any agent* achieving *Room selected* is required not to achieve *Prepayment made*, and any agent achieving *Prepayment made* is required not to achieve *Room selected*, when specifying a SoD constraint between these goals.
- *Any agent* achieving *eticket generated* is required not to achieve *credit card verified*, and any agent achieving *credit card verified* is required not to achieve *eticket generated*, when specifying a SoD constraint between these goals.
- *Any agent* achieving *Tickets booked* is required to achieve *Hotel booked* , and any agent achieving *Hotel booked* is required not to achieve *Tickets booked*, when specifying a CoD constraint between these goals.

Responsible	Security Requirement	Requester	Description
Hotel	no-delegation (Hotel booked)	Tourist	Hotel requires no-delegation for goal Hotel booked ,when delegating Hotel booked to Hotel.
	non-modification (Personal data)	Tourist	Tourist requires Hotel non-modification of Information Personal data.
	need-to-know (Personal data) (Hotel booked)	Tourist	Tourist requires Hotel need-to-know of Information Personal data, in the scope of goal Hotel booked .
Tourist	trustworthiness (Hotel, delegated(Tourist,Hotel, Hotel booked))	Tourist	Hotel shall provide proof of trustworthiness for Tourist to delegate him goal Hotel booked .
TAS	no-delegation (Tickets booked)	Tourist	TAS requires no-delegation for goal Tickets booked,when delegating Tickets booked to TAS.
	non-repudiation-of-acceptance (delegated(Tourist,TAS,Tickets booked))	Tourist	Tourist require non-repudiation-of-acceptance for goal Tickets booked,when delegating Tickets booked to TAS.
	non-production (Personal data,Itenerary)	Tourist	Tourist requires TAS non-production of Information Personal data and Itenerary.
	non-disclosure (Personal data,Itenerary)	Tourist	Tourist requires TAS non-disclosure of Information Personal data and Itenerary.
	need-to-know (Personal data,Itenerary) (Flight Ticket booked)	Tourist	Tourist requires TAS need-to-know of Information Personal data and Itenerary, in the scope of goal Flight Ticket booked.
Hotel Service	trustworthiness (Payment Service, delegated(Hotel Service,Payment Service,Prepayment made))	Hotel Service	Payment Service shall provide proof of trustworthiness for Hotel Service to delegate him goal Prepayment made.
Payment Service	not-reauthorized ({Itenerary},{},{R})	Amadeus Service	Amadeus Service wants Payment Service not to redistribute permissions on information {Itenerary} to other actors.
Amadeus Service	no-delegation (Flight Ticket booked)	TAS	Amadeus Service requires no-delegation for goal Flight Ticket booked,when delegating Flight Ticket booked to Amadeus Service.
	non-repudiation-of-acceptance (delegated(TAS,Amadeus	TAS	TAS require non-repudiation-of-acceptance for goal Flight Ticket

	Service,Flight Ticket booked))		booked,when delegating Flight Ticket booked to Amadeus Service.
	availability (Flight Ticket booked,90%)	TAS	TAS require Amadeus Service to assure an availability level of 90% for goal Flight Ticket booked.
	availability (Itinerary details,90%)	TAS	TAS require Amadeus Service to assure an availability level of 90% for document Itinerary details.
	receiver-integrity (transmitted(TAS,Amadeus Service,Itinerary details))	TAS	Amadeus Service shall ensure the integrity of transmission of the document Itinerary details being transmitted.
	need-to-know (Itenerary,Personal data) (Flight Ticket booked)	TAS	TAS requires Amadeus Service need-to-know of Information Itenerary and Personal data, in the scope of goal Flight Ticket booked.
	not-reauthorized ({Itenerary,Personal data},{Flight Ticket booked},{R})	TAS	TAS wants Amadeus Service not to redistribute permissions on information {Itenerary,Personal data} to other actors.
	not-reauthorized ({Itenerary,Personal data},{Flight Ticket booked},{P})	TAS	TAS wants Amadeus Service not to redistribute permissions on information {Itenerary,Personal data} to other actors.
"Any agents"	achieve-in-combination (Tickets booked,Tickets booked)	-	Any agent that achieves one of Tickets booked or Tickets booked, is required to achieve the other goal too.
	not-achieve-both (Room selected,Room selected)	-	Any agent that achieves Room selected or Room selected, is required not to achieve the other goal too.
	not-achieve-both (eticket generated,eticket generated)	-	Any agent that achieves eticket generated or eticket generated, is required not to achieve the other goal too.

Table 15 - Security Requirements for the Travel Agency Service Project

Table 16 summarises the authorizations actors in the Travel Agency Service project grant to one another.

Authorisor	Information	Goal	Allowed Operations	Denyed Operations	Authorisee	Description

Tourist	Personal data Itenerary	Flight Ticket booked	R	P, T	TAS	Transferable authority
	Itenerary Personal data		P, T		Amadeus Service	Transferable authority
	Personal data	Hotel booked	R	M	Hotel	Transferable authority
TAS	Itenerary Personal data	Flight Ticket booked	R, P		Amadeus Service	Non-transferable authority
Amadeus Service	Itenerary		R		Payment Service	Non-transferable authority

Table 16 - Authorizations in the Travel Agency Service project

Well-formedness Analysis

The purpose of well-formedness analysis is to verify whether the diagram for the project Travel Agency Service is consistent and valid. A diagram is considered to be consistent if its constituent elements (concepts and relationships) are drawn and interconnected following the semantics of the modelling language (STS-ml in our case). Thus, well-formedness analysis performs post checks to verify compliance with STS-ml semantics for all checks that cannot be performed live over the models.

More details about the performed checks and their purpose can be found in Appendix B.

The Well-formedness Analysis analysis for the Travel Agency Service has identified the problems summarised in Table 17.

Type	Category	Text	Description
WARN.	Delegation Child Cycle	Delegation loop	There is a delegation cycle created by the delegation of goal "Room selected", which is a subgoal of "Hotel booked ", back to "Hotel"

Table 17 - Well-formedness Analysis Analysis Results

Security Analysis

The purpose of security analysis is to verify whether the diagram for the project Travel Agency Service allows the satisfaction of the specified security needs or not. As a result, for all security needs expressed by stakeholders, it checks in the model whether there is any possibility for the security need to be violated. This analysis takes into account the semantics of STS-ml, defining the behaviour of the different elements represented in the models. The elements' behaviour is defined by propagation rules that consider what concepts and what relationships the specification of a given security need affects. Datalog is used to define the semantics of STS-ml to express facts (things always hold) and rules.

You can find more details about the performed checks in Appendix C.

The Security Analysis analysis for the Travel Agency Service has identified the problems summarised in Table 18.

Type	Category	Text	Description
ERROR	No_Delegation Violation check	"Hotel" makes an unauthorised redelegation of goal "Hotel booked "	"Tourist" has expressed a no_delegation security need over the delegation of the goal "Hotel booked " to "Hotel", and yet "Hotel" is re-delegating goal "Hotel booked " to "Hotel Service"
ERROR	No_Delegation Violation check	"TAS" makes an unauthorised redelegation of goal "Flight Ticket booked"	"Tourist" has expressed a no_delegation security need over the delegation of the goal "Tickets booked" to "TAS", and yet "TAS" is re-delegating goal "Flight Ticket booked" to "Amadeus Service"
ERROR	Non_Production Violation	"TAS" makes an unauthorised production of information "Schedule"	There is no authorization relationship towards "TAS" for information "Schedule", but "TAS" can produce "Schedule" since there is a produce relationship from its goal "Train Ticket booked" towards document "" representing "Schedule"
ERROR	Non_Production Violation	"TAS" makes an unauthorised production of information "Itenerary"	"Tourist" has required "TAS" non_production of information "Itenerary", but "TAS" can produce "Itenerary" since there is a produce relationship from its goal "Train Ticket booked" towards document "Tickets" representing "Itenerary"
ERROR	Non_Production Violation	"TAS" makes an unauthorised production of information "Destination"	There is no authorization relationship towards "TAS" for information "Destination", but "TAS" can produce "Destination" since there is a produce relationship from its goal "Train Ticket booked"

				towards document "" representing "Destination"
	ERROR	Non_Disclosure Violation	"TAS" makes an unauthorised distribution of information "Schedule"	There is no authorization relationship towards "TAS", but "TAS" is distributing "Schedule" to "Amadeus Service" by providing document "Itinerary details" to "Amadeus Service"
	ERROR	Non_Disclosure Violation	"TAS" makes an unauthorised distribution of information "Destination"	There is no authorization relationship towards "TAS", but "TAS" is distributing "Destination" to "Amadeus Service" by providing document "Itinerary details" to "Amadeus Service"
	ERROR	Non_Disclosure Violation	"TAS" makes an unauthorised distribution of information "Itenerary"	"Tourist" has required "TAS" non_disclosure of information "Itenerary", but "TAS" is distributing "Itenerary" to "Amadeus Service" by providing document "Itinerary details"
	ERROR	NTK Violation	"TAS" violates its authority performing operations in another goal scope	"Tourist" has required "TAS" need_to_know over information "Itenerary", requiring "TAS" not to perform any operations over "Itenerary" other than for "Flight Ticket booked", but "TAS" can perform operations over "Itenerary" for "Tickets booked", which is different from "Itenerary" and is not a subgoal of "Flight Ticket booked"
	ERROR	Explicit non-reauthorization	"Amadeus Service" violates its authority passing permissions without having the authority to transfer rights	"Amadeus Service" has no authority to transfer authority to other actors, but it still authorises "Itenerary"
	ERROR	Explicit non-reauthorization	"Amadeus Service" violates its authority passing permissions without having the authority to transfer rights	"Amadeus Service" has no authority to transfer authority to other actors, but it still authorises "Destination"
	ERROR	Explicit non-reauthorization	"Amadeus Service" violates its authority passing permissions without having the authority to transfer rights	"Amadeus Service" has no authority to transfer authority to other actors, but it still authorises "Schedule"
	ERROR	Non-reauthorization Violation: produce	"TAS" violates its authority passing permission to produce, in an unauthorised way	"TAS" has no authority to produce information "Personal data", but still authorises "Amadeus Service" to produce

			"Personal data"
ERROR	Non-reauthorization Violation: produce	"TAS" violates its authority passing permission to produce, in an unauthorised way	"TAS" has no authority to produce information "Itenerary", but still authorises "Amadeus Service" to produce "Itenerary"
ERROR	Non-reauthorization Violation: produce	"TAS" violates its authority passing permission to produce, in an unauthorised way	"TAS" has no authority to produce information "Schedule", but still authorises "Amadeus Service" to produce "Schedule"
ERROR	Non-reauthorization Violation: produce	"TAS" violates its authority passing permission to produce, in an unauthorised way	"TAS" has no authority to produce information "Destination", but still authorises "Amadeus Service" to produce "Destination"
ERROR	Sod Goal Violation	There is a separation of duty violation with respect to the goals "eticket generated" and "credit card verified"	Goal "eticket generated" and goal "credit card verified" should not be achieved by the same actor, since a separation of duty is expressed between these two goals, but "Amadeus Service" wants to achieve them both
ERROR	Bod Goal Violation	Possible violation of binding of duties between goals, there is no agent playing the roles	Goal "Tickets booked" and goal "Hotel booked " should be achieved by the same actor, since a binding of duty is expressed between these goals, but there is no actor to achieve them both
ERROR	Bod Goal Violation	Possible violation of binding of duties between goals, there is no agent playing the roles	Goal "Train Ticket booked" and goal "Hotel booked " should be achieved by the same actor, since a binding of duty is expressed between these goals, but there is no actor to achieve them both
ERROR	Bod Goal Violation	Possible violation of binding of duties between goals, there is no agent playing the roles	Goal "Tickets booked" and goal "Hotel booked " should be achieved by the same actor, since a binding of duty is expressed between these goals, but there is no actor to achieve them both
ERROR	Bod Goal Violation	Possible violation of binding of duties between goals, there is no agent playing the roles	Goal "Train Ticket booked" and goal "Hotel booked " should be achieved by the same actor, since a binding of duty is expressed between these goals, but there is no actor to achieve them both

Table 18 - Security Analysis Analysis Results

Secure business process models

This section describes the secure business process models, the security policies and the outcome of the verification analysis of security policies

Specifically, secure business process models specify business processes with security aspects.Security policies specify behaviours that shall or shall not be specified in the business process models.The verification analysis checks whether the security policies are satisfied against all secure business process models.

Secure business processes models

Business processes are sequences of actions executed by one or more technical components and/or people. Secure business process diagrams represent such business processes with an emphasis on security aspects. In the following, secure business processes models of "Travel Agency Service" project are described.

Diagram: "Trip planned Process"

Figure 5 (a larger picture is shown in appendix D) shows "Trip planned Process" diagram, which consists of 1process. Such business process is composed of 4 activities, 4 events, 2 gateways. They are executed by 2 participants.

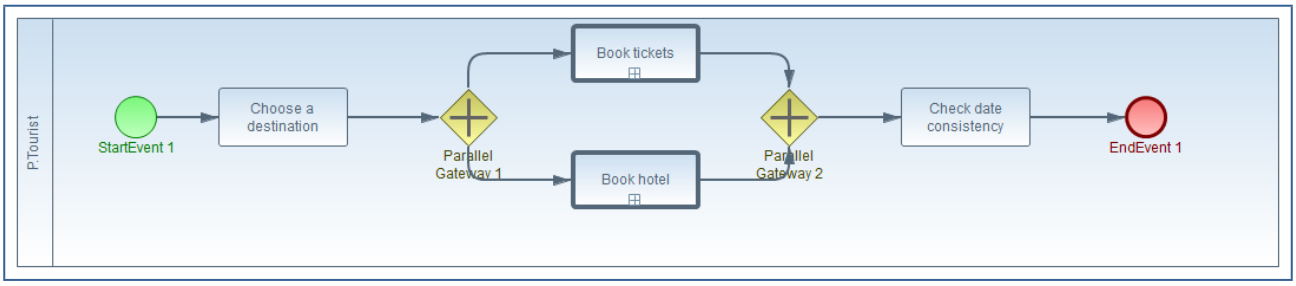

Figure 4 - "Trip planned Process" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Tourist	Participant		

Table 19 - Participants for diagram "Trip planned Process"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Choose a destination	Task	
Check date consistency	Task	

Table 20 - Tasks for diagram "Trip planned Process"

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is

interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Book tickets	Tickets booked delegation	
Book hotel	Hotel booked delegation	

Table 21 - Call activities for diagram "Trip planned Process"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 1	Start		
EndEvent 1	End		

Table 22 - Events for diagram "Trip planned Process"

Gateways

Gateways are used to branch business process in multiple flows that can be executed exclusively or in parallel, accordingly to the type of gateway. Each gateway can split the execution flow (diverging gateways), merge two or more execution flows (converging gateways), or both merge and split control flows (mixed gateways).

Name	Type	Direction	Description
Parallel Gateway 1	ParallelGateway	Unspecified	
Parallel Gateway 2	ParallelGateway	Unspecified	

Table 23 - Gateways for diagram "Trip planned Process"

Diagram: "Tickets booked delegation"

Figure 5 (a larger picture is shown in appendix D) shows "Tickets booked delegation" diagram, which consists of 2processes. Such business processes are composed of 7 activities, 7 events, 2 gateways. They are executed by 3 participants.

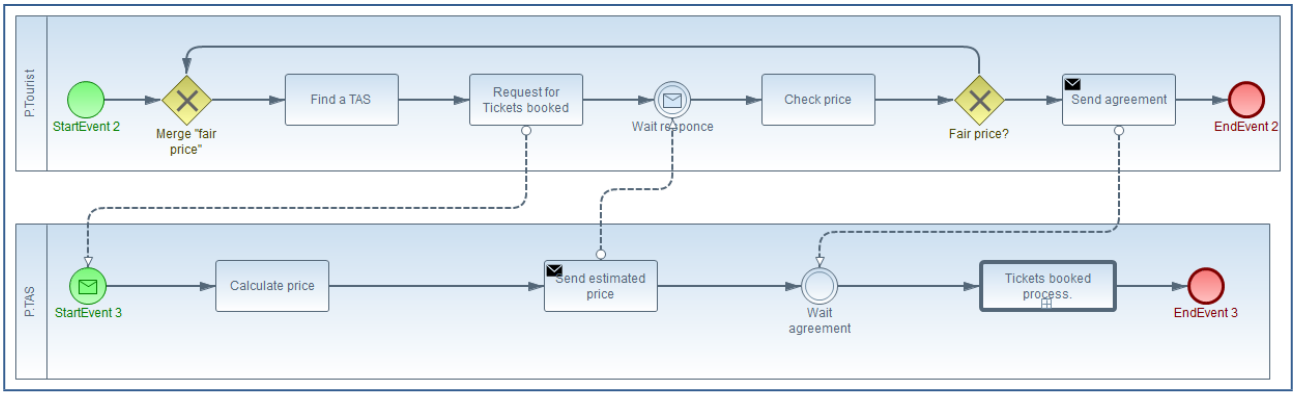

Figure 6 - "Tickets booked delegation" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Tourist	Participant		
P.TAS	Participant		

Table 24 - Participants for diagram "Tickets booked delegation"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Request for Tickets booked	Task	
Find a TAS	Task	
Check price	Task	
Send agreement	Task	
Calculate price	Task	
Send estimated price	Task	

Table 25 - Tasks for diagram "Tickets booked delegation"

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Tickets booked process.	TAS Reads Travelling Order	

Table 26 - Call activities for diagram "Tickets booked delegation"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 2	Start		

EndEvent 2	End	
Wait responce	Intermediate catch	Message
StartEvent 3	Start	Message
EndEvent 3	End	
Wait agreement	Intermediate catch	

Table 27 - Events for diagram "Tickets booked delegation"

Gateways

Gateways are used to branch business process in multiple flows that can be executed exclusively or in parallel, accordingly to the type of gateway. Each gateway can split the execution flow (diverging gateways), merge two or more execution flows (converging gateways), or both merge and split control flows (mixed gateways).

Name	Type	Direction	Description
Fair price?	Exclusive	Unspecified	
Merge "fair price"	Exclusive	Unspecified	

Table 28 - Gateways for diagram "Tickets booked delegation"

Diagram: "TAS Reads Travelling Order "

Figure 5 shows "TAS Reads Travelling Order " diagram, which consists of 1process. Such business process is composed of 3 activities, 3 events, 1 data object, 2 gateways. They are executed by 2 participants.

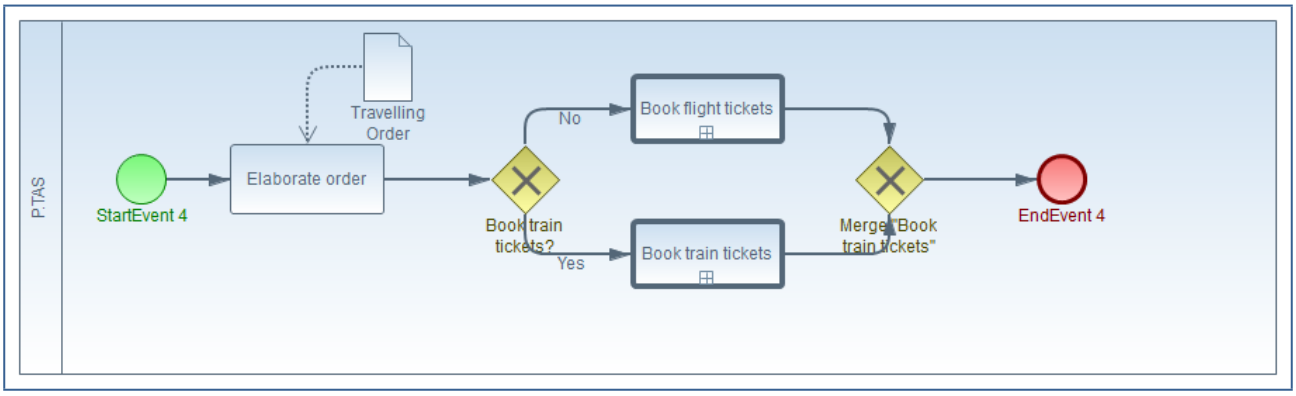

Figure 7 - "TAS Reads Travelling Order " Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.TAS	Participant		

Table 29 - Participants for diagram "TAS Reads Travelling Order "

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Elaborate order	Task	

Table 30 - Tasks for diagram "TAS Reads Travelling Order "

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Book flight tickets	TAS Produces Tickets	
Book train tickets	Flight Ticket booked delegation	

Table 31 - Call activities for diagram "TAS Reads Travelling Order "

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 4	Start		
EndEvent 4	End		

Table 32 - Events for diagram "TAS Reads Travelling Order "

Gateways

Gateways are used to branch business process in multiple flows that can be executed exclusively or in parallel, accordingly to the type of gateway. Each gateway can split the execution flow (diverging gateways), merge two or more execution flows (converging gateways), or both merge and split control flows (mixed gateways).

Name	Type	Direction	Description
Book train tickets?	Exclusive	Unspecified	
Merge "Book train tickets"	Exclusive	Unspecified	

Table 33 - Gateways for diagram "TAS Reads Travelling Order "

Data Elements

Data elements represent data in the managed by the business process, i.e. required for their execution or produced by their execution.

Name	Type	Description
Travelling Order	Data Object	

Table 34 - Data elements for diagram "TAS Reads Travelling Order "

Diagram: "TAS Produces Tickets"

Figure 5 shows "TAS Produces Tickets" diagram, which consists of 1process. Such business process is composed of 1 activity, 1 event, 1 data object, They are executed by 2 participants.

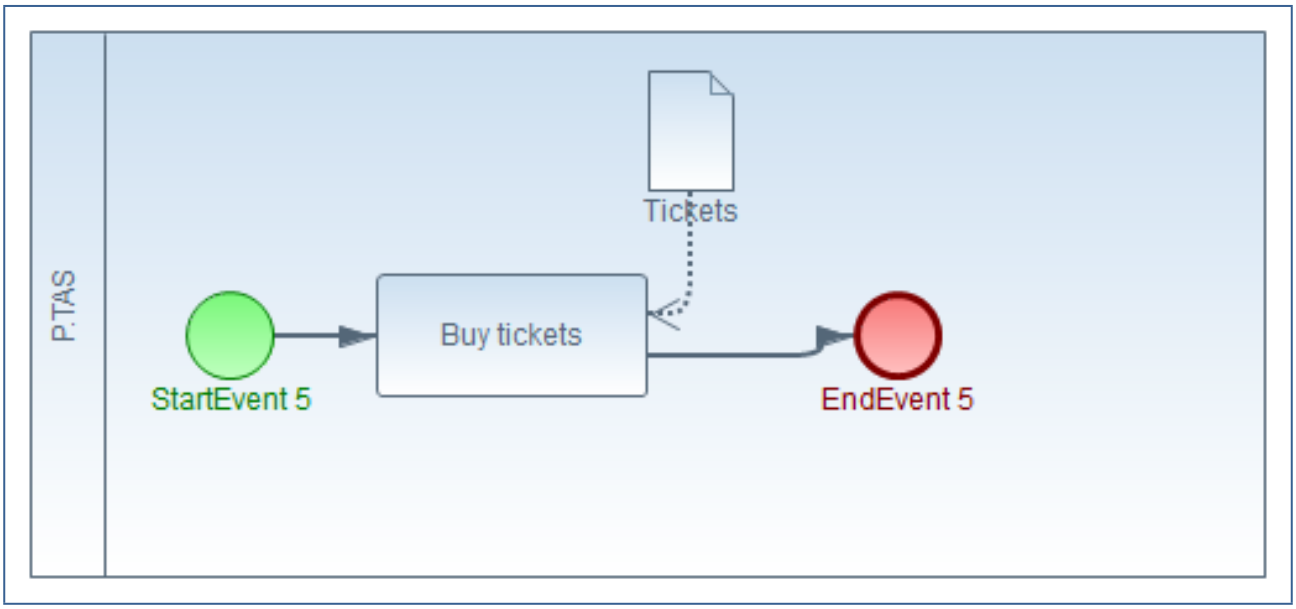

Figure 8 - "TAS Produces Tickets" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.TAS	Participant		

Table 35 - Participants for diagram "TAS Produces Tickets"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Buy tickets	Task	

Table 36 - Tasks for diagram "TAS Produces Tickets"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 5	Start		
EndEvent 5	End		

Table 37 - Events for diagram "TAS Produces Tickets"

Data Elements

Data elements represent data in the managed by the business process, i.e. required for their execution or produced by their execution.

Name	Type	Description
Tickets	Data Object	

Table 38 - Data elements for diagram "TAS Produces Tickets"

Diagram: "Flight Ticket booked delegation"

Figure 5 shows "Flight Ticket booked delegation" diagram, which consists of 2processes. Such business processes are composed of 2 activities, 2 events, They are executed by 3 participants.

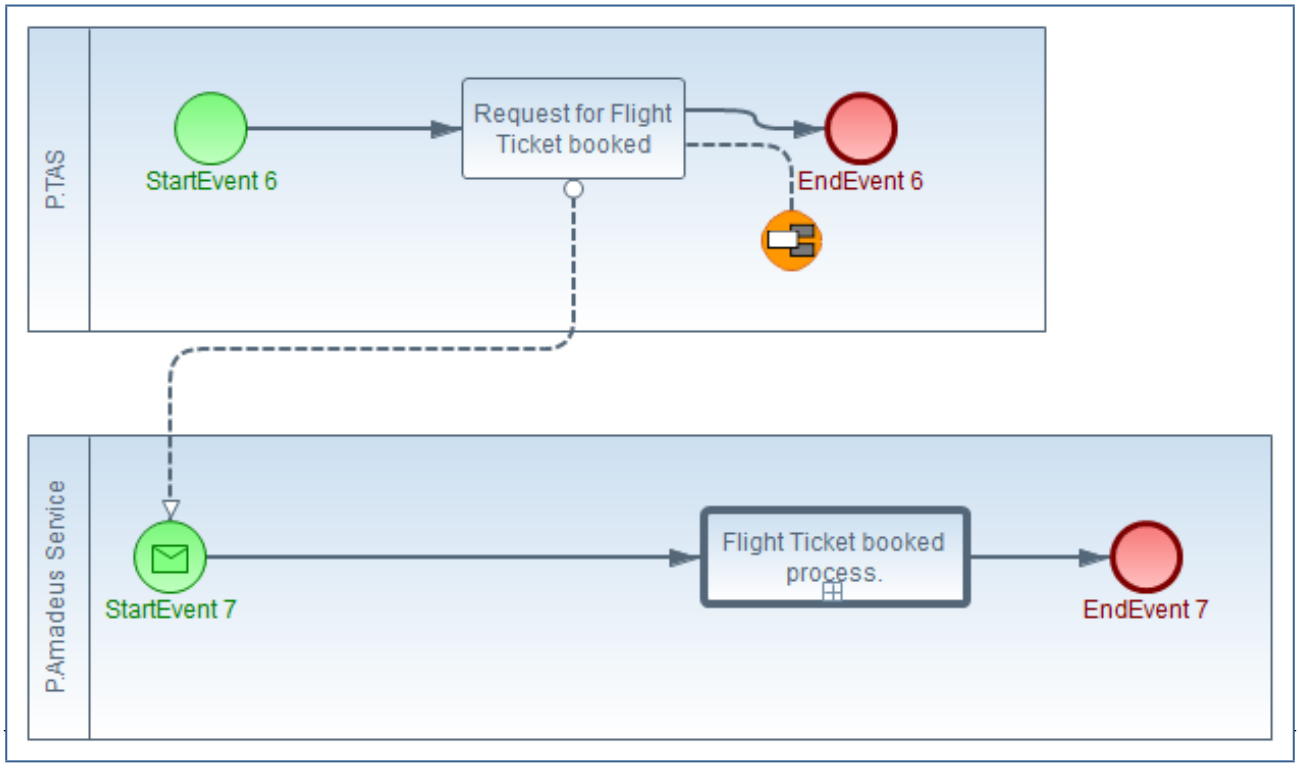

Figure 9 - "Flight Ticket booked delegation" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.TAS	Participant		
P.Amadeus Service	Participant		

Table 39 - Participants for diagram "Flight Ticket booked delegation"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Request for Flight Ticket booked	Task	

Table 40 - Tasks for diagram "Flight Ticket booked delegation"

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Flight Ticket booked process.	Flight Ticket booked Process	

Table 41 - Call activities for diagram "Flight Ticket booked delegation"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 6	Start		
EndEvent 6	End		
StartEvent 7	Start	Message	
EndEvent 7	End		

Table 42 - Events for diagram "Flight Ticket booked delegation"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Non-delegation

We defined the security aspect represented by this security annotation as the ability of the system to require that a set of actions is executed only by the users assigned.

Table 43 enlists the non-delegation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Request for Flight Ticket booked	Enforced by		

Table 43 - "Non-delegation security annotation for diagram Flight Ticket booked delegation

Diagram: "Flight Ticket booked Process"

Figure 5 (a larger picture is shown in appendix D) shows "Flight Ticket booked Process" diagram, which consists of 1process. Such business process is composed of 4 activities, 4 events, 1 gateway. They are executed by 2 participants.

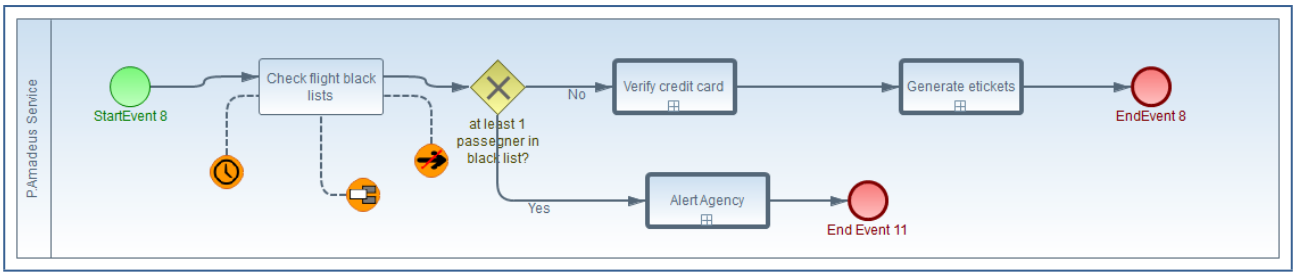

Figure 10 - "Flight Ticket booked Process" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Amadeus Service	Participant		

Table 44 - Participants for diagram "Flight Ticket booked Process"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description

Check flight black lists	Task

Table 45 - Tasks for diagram "Flight Ticket booked Process"

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Generate etickets	Amadeus Service Produces Flight tickets	
Verify credit card	credit card verified Process	
Alert Agency	Alert agency process	

Table 46 - Call activities for diagram "Flight Ticket booked Process"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 8	Start		
EndEvent 8	End		
End Event 11	End		

Table 47 - Events for diagram "Flight Ticket booked Process"

Gateways

Gateways are used to branch business process in multiple flows that can be executed exclusively or in parallel, accordingly to the type of gateway. Each gateway can split the execution flow (diverging gateways), merge two or more execution flows (converging gateways), or both merge and split control flows (mixed gateways).

Name	Type	Direction	Description
at least 1 passegner in black list?	Exclusive	Unspecified	

Table 48 - Gateways for diagram "Flight Ticket booked Process"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Availability

We defined the security aspect represented by this security annotation as the ability of a system to ensure that all system's components are available and operational when they are required by authorized users.

Table 49 enlists the availability security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Check flight black lists	Enforced by		
	Level	0.0	
	Authorized end users		

Table 49 - "Availability security annotation for diagram Flight Ticket booked Process

Non-repudiation

We defined the security aspect represented by this security annotation as the ability of a system to prove (with legal validity) occurrence/non-occurrence of an event or participation/non-participation of a party in an event.

Table 50 enlists the non-repudiation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Check flight black lists	Enforced by		
	Execution	Not Specified	

Table 50 - "Non-repudiation security annotation for diagram Flight Ticket booked Process

Non-delegation

We defined the security aspect represented by this security annotation as the ability of the system to require that a set of actions is executed only by the users assigned.

Table 51 enlists the non-delegation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Check flight black lists	Enforced by		

Table 51 - "Non-delegation security annotation for diagram Flight Ticket booked Process

Diagram: "credit card verified Process"

Figure 5 (a larger picture is shown in appendix D) shows "credit card verified Process" diagram, which consists of 1process. Such business process is composed of 3 activities, 3 events, 1 gateway. They are executed by 2 participants.

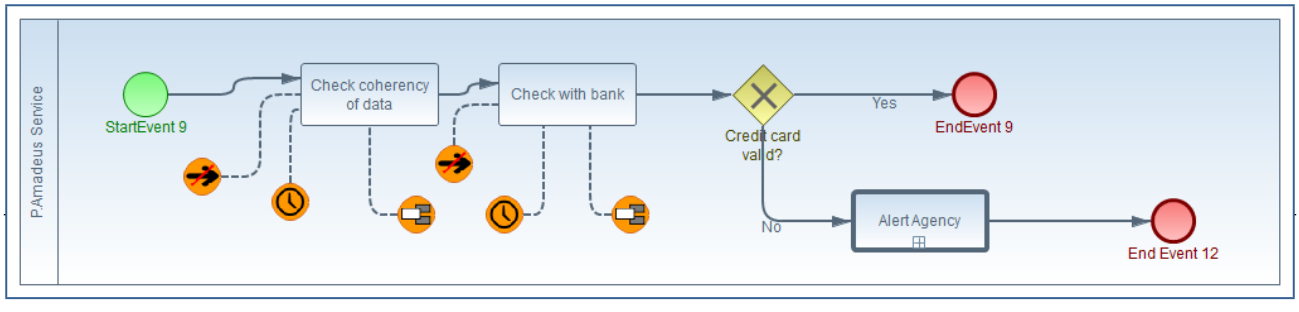

Figure 11 - "credit card verified Process" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Amadeus Service	Participant		

Table 52 - Participants for diagram "credit card verified Process"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Check coherency of data	Task	
Check with bank	Task	

Table 53 - Tasks for diagram "credit card verified Process"

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Alert Agency	Alert agency process	

Table 54 - Call activities for diagram "credit card verified Process"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 9	Start		
EndEvent 9	End		
End Event 12	End		

Table 55 - Events for diagram "credit card verified Process"

Gateways

Gateways are used to branch business process in multiple flows that can be executed exclusively or in parallel, accordingly to the type of gateway. Each gateway can split the execution flow (diverging gateways), merge two or more execution flows (converging gateways), or both merge and split control flows (mixed gateways).

Name	Type	Direction	Description
Credit card valid?	Exclusive	Unspecified	

Table 56 - Gateways for diagram "credit card verified Process"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Availability

We defined the security aspect represented by this security annotation as the ability of a system to ensure that all system's components are available and operational when they are required by authorized users.

Table 57 enlists the availability security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Check coherency of data	Enforced by		
	Level	0.0	
	Authorized end users		
Check with bank	Enforced by		
	Level	0.0	
	Authorized end users		

Table 57 - "Availability security annotation for diagram credit card verified Process

Non-repudiation

We defined the security aspect represented by this security annotation as the ability of a system to prove (with legal validity) occurrence/non-occurrence of an event or participation/non-participation of a party in an event.

Table 58 enlists the non-repudiation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Check coherency of data	Enforced by		
	Execution	Not Specified	
Check with bank	Enforced by		
	Execution	Not Specified	

Table 58 - "Non-repudiation security annotation for diagram credit card verified Process

Non-delegation

We defined the security aspect represented by this security annotation as the ability of the system to require that a set of actions is executed only by the users assigned.

Table 59 enlists the non-delegation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Check coherency of data	Enforced by		
Check with bank	Enforced by		

Table 59 - "Non-delegation security annotation for diagram credit card verified Process

Diagram: "Amadeus Service Produces Flight tickets"

Figure 5 shows "Amadeus Service Produces Flight tickets" diagram, which consists of 1process. Such business process is composed of 1 activity, 1 event, 2 data objects, They are executed by 2 participants.

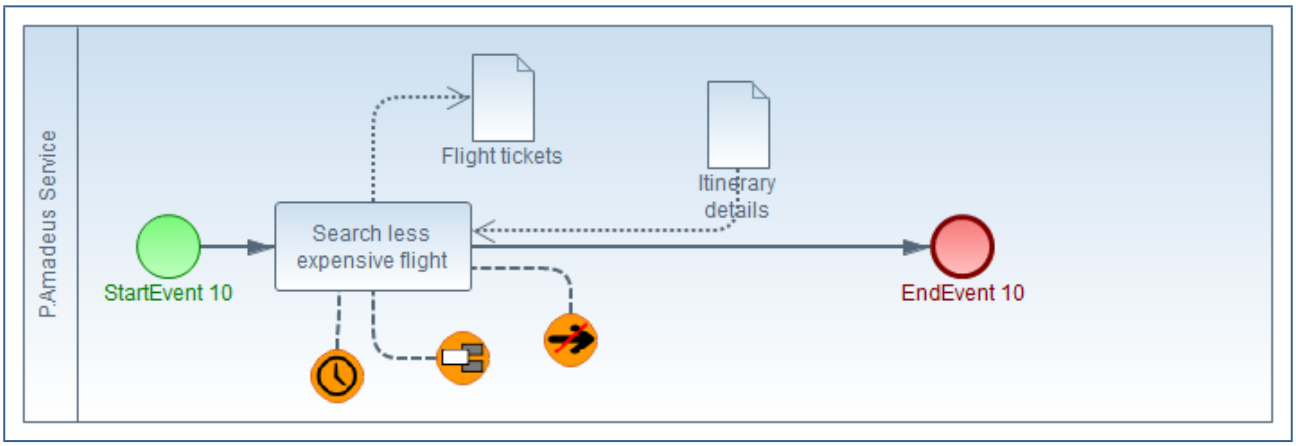

Figure 12 - "Amadeus Service Produces Flight tickets" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Amadeus Service	Participant		

Table 60 - Participants for diagram "Amadeus Service Produces Flight tickets"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description

Search less expensive flight	Task

Table 61 - Tasks for diagram "Amadeus Service Produces Flight tickets"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 10	Start		
EndEvent 10	End		

Table 62 - Events for diagram "Amadeus Service Produces Flight tickets"

Data Elements

Data elements represent data in the managed by the business process, i.e. required for their execution or produced by their execution.

Name	Type	Description
Flight tickets	Data Object	
Itinerary details	Data Object	

Table 63 - Data elements for diagram "Amadeus Service Produces Flight tickets"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Availability

We defined the security aspect represented by this security annotation as the ability of a system to ensure that all system's components are available and operational when they are required by authorized users.

Table 64 enlists the availability security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Search less expensive flight	Enforced by		
	Level	0.0	
	Authorized end users		

Table 64 - "Availability security annotation for diagram Amadeus Service Produces Flight tickets

Non-repudiation

We defined the security aspect represented by this security annotation as the ability of a system to prove (with legal validity) occurrence/non-occurrence of an event or participation/non-participation of a party in an event.

Table 65 enlists the non-repudiation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Search less expensive flight	Enforced by		
	Execution	Not Specified	

Table 65 - "Non-repudiation security annotation for diagram Amadeus Service Produces Flight tickets

Non-delegation

We defined the security aspect represented by this security annotation as the ability of the system to require that a set of actions is executed only by the users assigned.

Table 66 enlists the non-delegation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Search less expensive flight	Enforced by		

Table 66 - "Non-delegation security annotation for diagram Amadeus Service Produces Flight tickets

Diagram: "Hotel booked delegation"

Figure 5 (a larger picture is shown in appendix D) shows "Hotel booked delegation" diagram, which consists of 2processes. Such business processes are composed of 4 activities, 4 events, 1 gateway. They are executed by 3 participants.

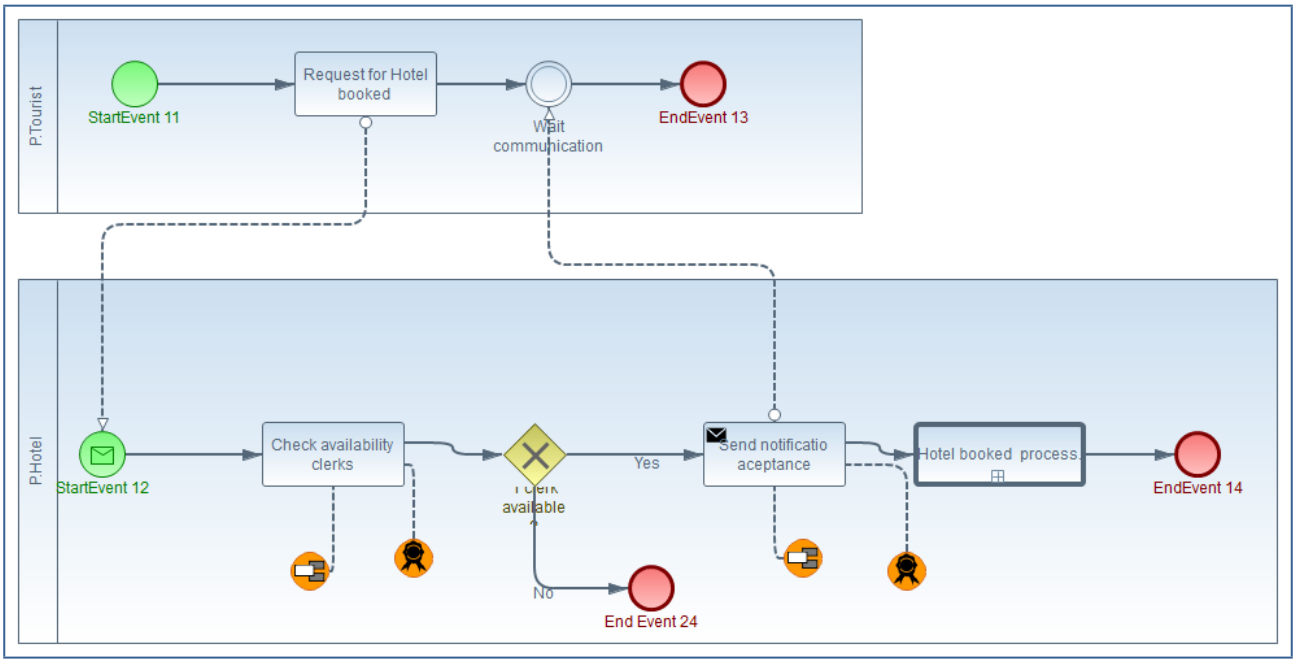

Figure 13 - "Hotel booked delegation" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description

P.Tourist	Participant
P.Hotel	Participant

Table 67 - Participants for diagram "Hotel booked delegation"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Request for Hotel booked	Task	
Check availability clerks	Task	
Send notificatio aceptance	Task	

Table 68 - Tasks for diagram "Hotel booked delegation"

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Hotel booked process.	Hotel booked delegation 2	

Table 69 - Call activities for diagram "Hotel booked delegation"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 11	Start		
EndEvent 13	End		
Wait communication	Intermediate catch		
StartEvent 12	Start	Message	
EndEvent 14	End		
End Event 24	End		

Table 70 - Events for diagram "Hotel booked delegation"

Gateways

Gateways are used to branch business process in multiple flows that can be executed exclusively or in parallel, accordingly to the type of gateway. Each gateway can split the execution flow (diverging gateways), merge two or more execution flows (converging gateways), or both merge and split control flows (mixed gateways).

Name	Type	Direction	Description
1 clerk available?	Exclusive	Unspecified	

Table 71 - Gateways for diagram "Hotel booked delegation"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Authenticity

We defined the security aspect represented by this security annotation as the ability of a system to verify identity and establish trust in a third party and in information it provides.

Table 72 enlists the authenticity security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Check availability clerks	Enforced by		
	Identification	False	
	Authentication	False	
	Trust value	0.0	
Send notificatio aceptance	Enforced by		
	Identification	False	
	Authentication	False	
	Trust value	0.0	

Table 72 - "Authenticity security annotation for diagram Hotel booked delegation

Non-delegation

We defined the security aspect represented by this security annotation as the ability of the system to require that a set of actions is executed only by the users assigned.

Table 73 enlists the non-delegation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Check availability clerks	Enforced by		
Send notificatio aceptance	Enforced by		

Table 73 - "Non-delegation security annotation for diagram Hotel booked delegation

Diagram: "Hotel booked delegation 2"

Figure 5 shows "Hotel booked delegation 2" diagram, which consists of 2processes. Such business processes are composed of 2 activities, 2 events, They are executed by 3 participants.

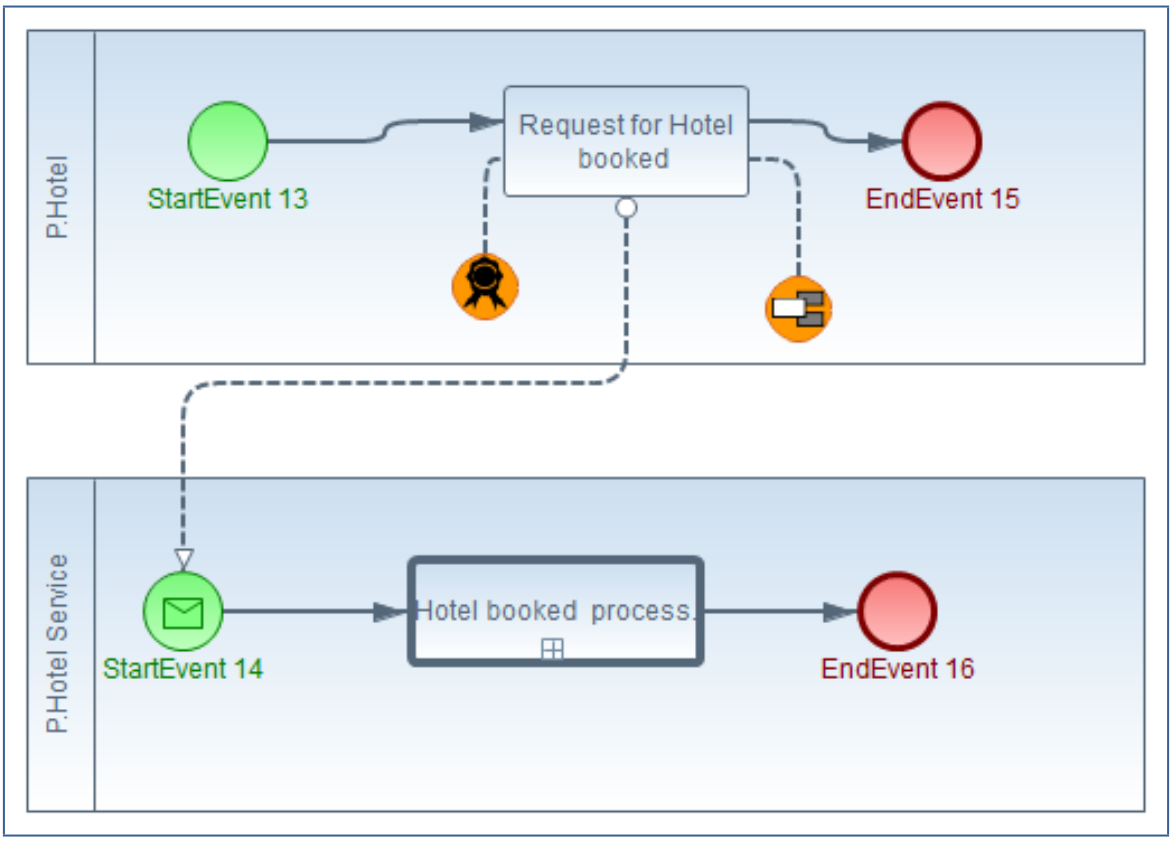

Figure 14 - "Hotel booked delegation 2" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Hotel	Participant		
P.Hotel Service	Participant		

Table 74 - Participants for diagram "Hotel booked delegation 2"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Request for Hotel booked	Task	

Table 75 - Tasks for diagram "Hotel booked delegation 2"

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Hotel booked process.	Hotel booked Process	

Table 76 - Call activities for diagram "Hotel booked delegation 2"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 13	Start		
EndEvent 15	End		
StartEvent 14	Start	Message	
EndEvent 16	End		

Table 77 - Events for diagram "Hotel booked delegation 2"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Authenticity

We defined the security aspect represented by this security annotation as the ability of a system to verify identity and establish trust in a third party and in information it provides.

Table 78 enlists the authenticity security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Request for Hotel booked	Enforced by		
	Identification	False	
	Authentication	False	
	Trust value	0.0	

Table 78 - "Authenticity security annotation for diagram Hotel booked delegation 2

Non-delegation

We defined the security aspect represented by this security annotation as the ability of the system to require that a set of actions is executed only by the users assigned.

Table 79 enlists the non-delegation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Request for Hotel booked	Enforced by		

Table 79 - "Non-delegation security annotation for diagram Hotel booked delegation 2

Diagram: "Hotel booked Process"

Figure 5 (a larger picture is shown in appendix D) shows "Hotel booked Process" diagram, which consists of 1process. Such business process is composed of 3 activities, 3 events, 3 gateways. They are executed by 2 participants.

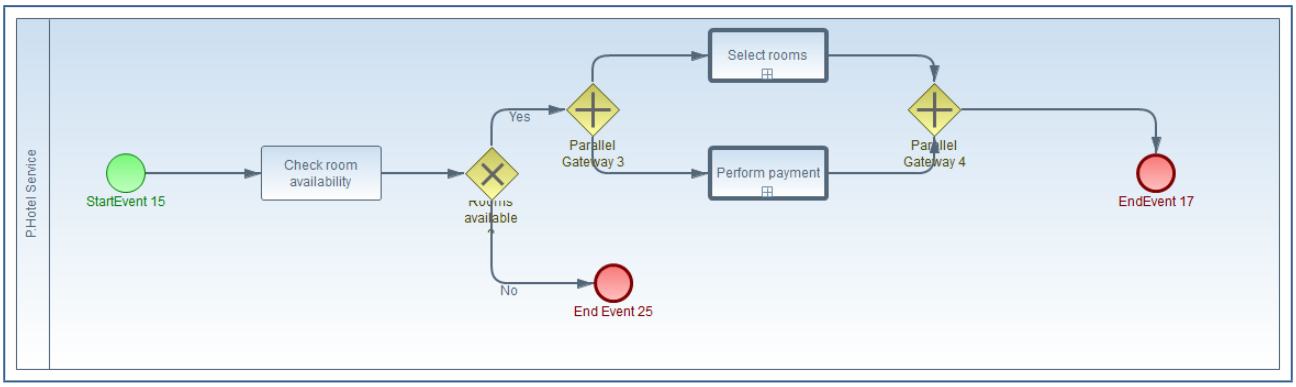

Figure 15 - "Hotel booked Process" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Hotel Service	Participant		

Table 80 - Participants for diagram "Hotel booked Process"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Check room availability	Task	

Table 81 - Tasks for diagram "Hotel booked Process"

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is

interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Select rooms	Room selected delegation	
Perform payment	Prepayment made delegation	

Table 82 - Call activities for diagram "Hotel booked Process"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 15	Start		
EndEvent 17	End		
End Event 25	End		

Table 83 - Events for diagram "Hotel booked Process"

Gateways

Gateways are used to branch business process in multiple flows that can be executed exclusively or in parallel, accordingly to the type of gateway. Each gateway can split the execution flow (diverging gateways), merge two or more execution flows (converging gateways), or both merge and split control flows (mixed gateways).

Name	Type	Direction	Description
Rooms available?	Exclusive	Unspecified	
Parallel Gateway 3	ParallelGateway	Unspecified	
Parallel Gateway 4	ParallelGateway	Unspecified	

Table 84 - Gateways for diagram "Hotel booked Process"

Diagram: "Prepayment made delegation"

Figure 5 shows "Prepayment made delegation" diagram, which consists of 2processes. Such business processes are composed of 2 activities, 2 events, They are executed by 3 participants.

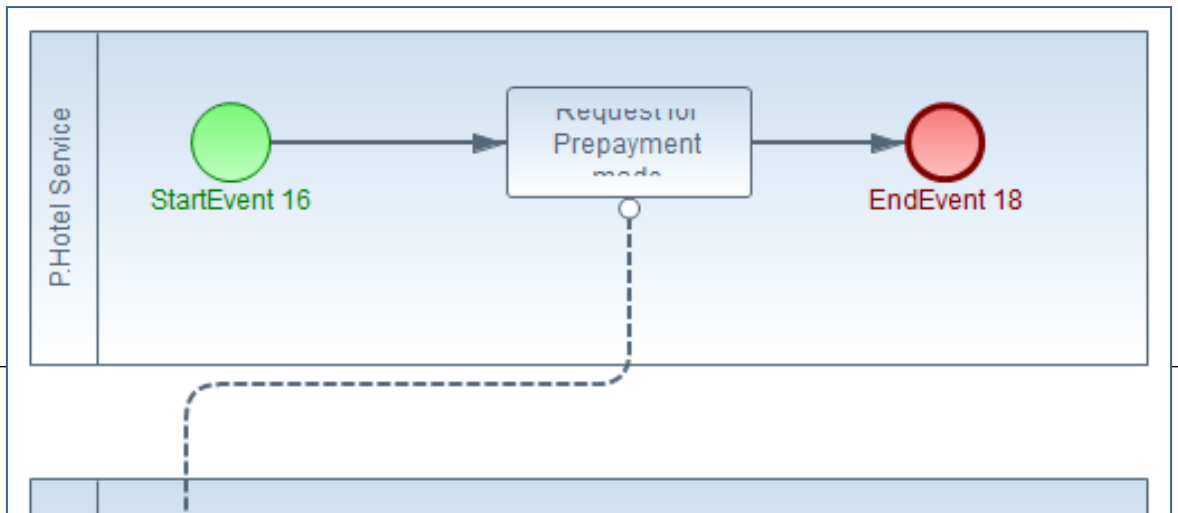

Figure 16 - "Prepayment made delegation" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Hotel Service	Participant		
P.Payment Service	Participant		

Table 85 - Participants for diagram "Prepayment made delegation"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Request for Prepayment made	Task	

Table 86 - Tasks for diagram "Prepayment made delegation"

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Prepayment made process.	Prepayment made Process	

Table 87 - Call activities for diagram "Prepayment made delegation"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 16	Start		
EndEvent 18	End		
StartEvent 17	Start	Message	
EndEvent 19	End		

Table 88 - Events for diagram "Prepayment made delegation"

Diagram: "Room selected delegation"

Figure 5 shows "Room selected delegation" diagram, which consists of 2processes. Such business processes are composed of 2 activities, 2 events, They are executed by 3 participants.

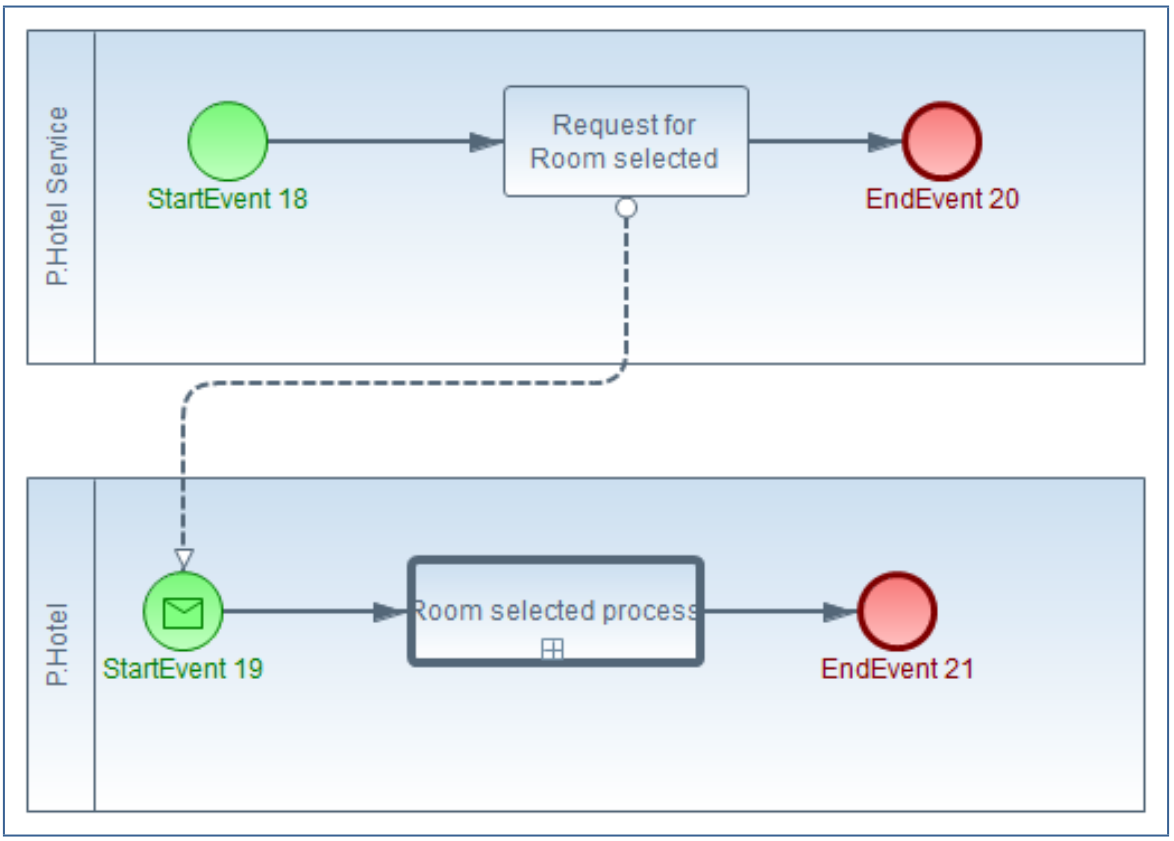

Figure 17 - "Room selected delegation" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Hotel Service	Participant		
P.Hotel	Participant		

Table 89 - Participants for diagram "Room selected delegation"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Request for Room selected	Task	

Table 90 - Tasks for diagram "Room selected delegation"

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Room selected process	Room selected Process	

Table 91 - Call activities for diagram "Room selected delegation"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 18	Start		
EndEvent 20	End		
StartEvent 19	Start	Message	
EndEvent 21	End		

Table 92 - Events for diagram "Room selected delegation"

Diagram: "Prepayment made Process"

Figure 5 (a larger picture is shown in appendix D) shows "Prepayment made Process" diagram, which consists of 1process. Such business process is composed of 3 activities, 3 events, 2 gateways. They are executed by 2 participants.

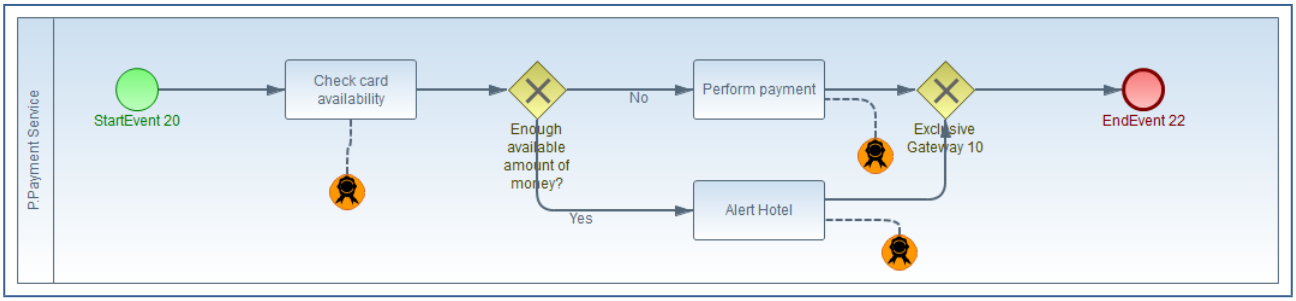

Figure 18 - "Prepayment made Process" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Payment Service	Participant		

Table 93 - Participants for diagram "Prepayment made Process"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Check card availability	Task	
Perform payment	Task	
Alert Hotel	Task	

Table 94 - Tasks for diagram "Prepayment made Process"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 20	Start		
EndEvent 22	End		

Table 95 - Events for diagram "Prepayment made Process"

Gateways

Gateways are used to branch business process in multiple flows that can be executed exclusively or in parallel, accordingly to the type of gateway. Each gateway can split the execution flow (diverging gateways), merge two or more execution flows (converging gateways), or both merge and split control flows (mixed gateways).

Name	Type	Direction	Description
Enough available amount of money?	Exclusive	Unspecified	
Exclusive Gateway 10	Exclusive	Unspecified	

Table 96 - Gateways for diagram "Prepayment made Process"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Authenticity

We defined the security aspect represented by this security annotation as the ability of a system to verify identity and establish trust in a third party and in information it provides.

Table 97 enlists the authenticity security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Check card availability	Enforced by		
	Identification	False	
	Authentication	False	
	Trust value	0.0	
Perform payment	Enforced by		
	Identification	False	
	Authentication	False	
	Trust value	0.0	
Alert Hotel	Enforced by		
	Identification	False	
	Authentication	False	
	Trust value	0.0	

Table 97 - "Authenticity security annotation for diagram Prepayment made Process

Diagram: "Room selected Process"

Figure 5 shows "Room selected Process" diagram, which consists of 1process. Such business process is composed of 2 activities, 2 events, They are executed by 2 participants.

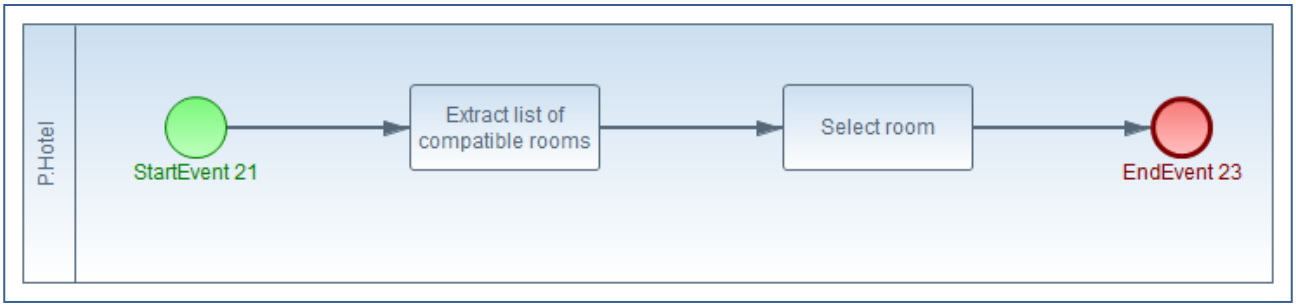

Figure 19 - "Room selected Process" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.Hotel	Participant		

Table 98 - Participants for diagram "Room selected Process"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Extract list of compatible rooms	Task	
Select room	Task	

Table 99 - Tasks for diagram "Room selected Process"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 21	Start		
EndEvent 23	End		

Table 100 - Events for diagram "Room selected Process"

Diagram: "Alert agency process"

Figure 5 shows "Alert agency process" diagram, which consists of 2processes. Such business processes are composed of 2 activities, 2 events, They are executed by 3 participants.

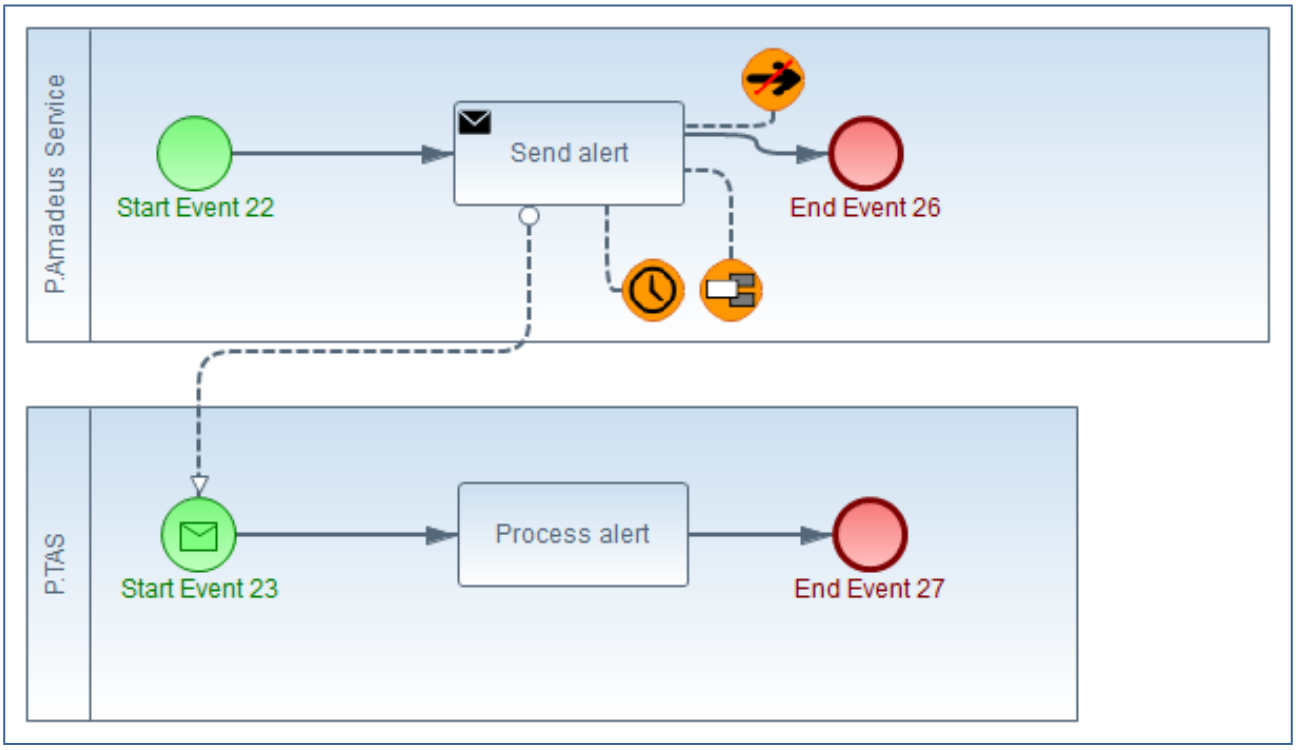

Figure 20 - "Alert agency process" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
Participant 37	Participant		

P.Amadeus Service	Participant
P.TAS	Participant

Table 101 - Participants for diagram "Alert agency process"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Send alert	Task	
Process alert	Task	

Table 102 - Tasks for diagram "Alert agency process"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
Start Event 22	Start		
End Event 26	End		
Start Event 23	Start	Message	
End Event 27	End		

Table 103 - Events for diagram "Alert agency process"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Availability

We defined the security aspect represented by this security annotation as the ability of a system to ensure that all system's components are available and operational when they are required by authorized users.

Table 104 enlists the availability security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Send alert	Enforced by		
	Level	0.0	

	Authorized end users

Table 104 - "Availability security annotation for diagram Alert agency process

Non-repudiation

We defined the security aspect represented by this security annotation as the ability of a system to prove (with legal validity) occurrence/non-occurrence of an event or participation/non-participation of a party in an event.

Table 105 enlists the non-repudiation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Send alert	Enforced by		
	Execution	Not Specified	

Table 105 - "Non-repudiation security annotation for diagram Alert agency process

Non-delegation

We defined the security aspect represented by this security annotation as the ability of the system to require that a set of actions is executed only by the users assigned.

Table 106 enlists the non-delegation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Send alert	Enforced by		

Table 106 - "Non-delegation security annotation for diagram Alert agency process

Diagram: "Itinerary details Transmission"

Figure 5 shows "Itinerary details Transmission" diagram, which consists of 2processes. Such business processes are composed of 2 activities, 2 events, They are executed by 3 participants.

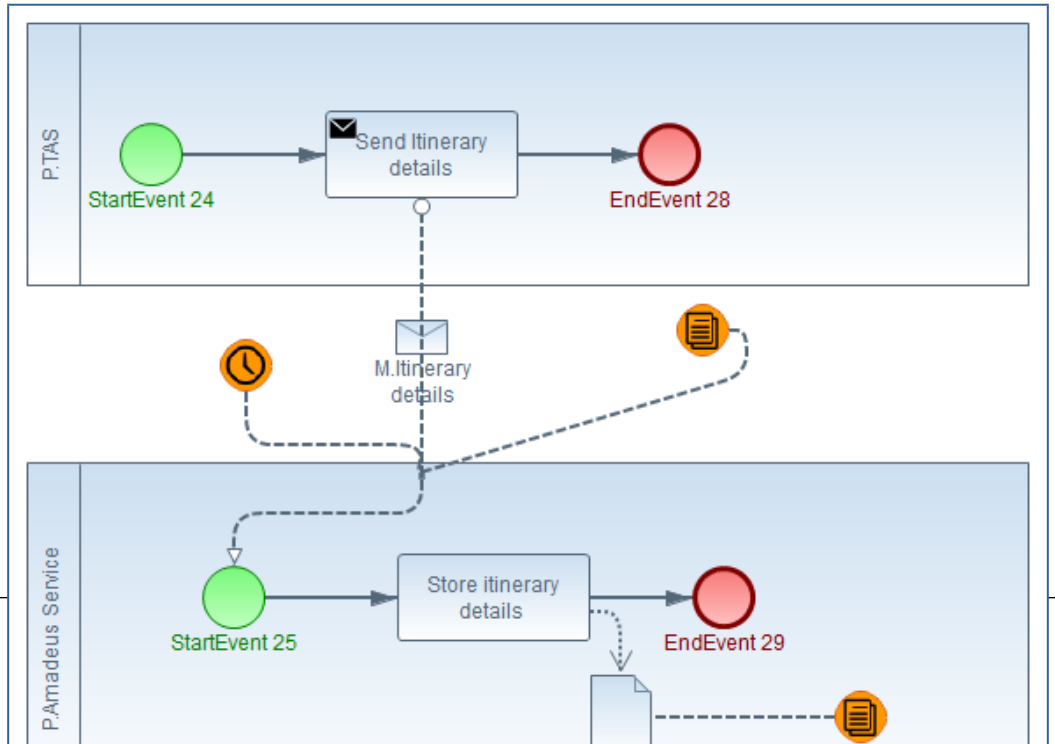

Figure 21 - "Itinerary details Transmission" Diagram

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
P.TAS	Participant		
P.Amadeus Service	Participant		

Table 107 - Participants for diagram "Itinerary details Transmission"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
Send Itinerary details	Task	
Store itinerary details	Task	

Table 108 - Tasks for diagram "Itinerary details Transmission"

Events

Events catch or throw global events in the system. They are used to start, interrupt or end a business process. Each event handles specific events, specified in its definition.

Name	Type	Definition	Description
StartEvent 24	Start		
EndEvent 28	End		
StartEvent 25	Start		
EndEvent 29	End		

Table 109 - Events for diagram "Itinerary details Transmission"

Data Elements

Data elements represent data in the managed by the business process, i.e. required for their execution or produced by their execution.

Name	Type	Description

Table 110 - Data elements for diagram "Itinerary details Transmission"

Messages transmissions

Message transmissions represent the communication of messages through message flows between participants.Messages can be used in more than one message transmission, we, therefore, specify all the messages of "Itinerary details Transmission" diagram in Table 111 and the all the message flows of "Itinerary details Transmission" diagram in Table Table 112.

Messages

Messages are the content of the flow of information between two participants.

Name	Description
M.Itinerary details	

Table 111 - Messages for diagram "Itinerary details Transmission"

Message flows

Message flows represent the communication channel between two SecBPMN2 elements.

Message Name	Source	Destination	Description
M.Itinerary details	Send Itinerary details	StartEvent 25	

Table 113 - "Itinerary details Transmission" message flows

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Availability

We defined the security aspect represented by this security annotation as the ability of a system to ensure that all system's components are available and operational when they are required by authorized users.

Table 114 enlists the availability security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Message Flow from "Send Itinerary details" to "StartEvent 25"	Enforced by		
	Level	0.0	
	Authorized end users		

Table 114 - "Availability security annotation for diagram Itinerary details Transmission

Integrity

We defined the security aspect represented by this security annotation as the ability of a system to ensure completeness, accuracy and absence of unauthorized modifications in all its components.

Table 115 enlists the integrity security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description

Message Flow from "Send Itinerary details" to "StartEvent 25"	Enforced by	
	Personnel	False
	Hardware	False
	Software	False
Itinerary details	Enforced by	
	Personnel	False
	Hardware	False
	Software	False

Table 115 - "Integrity security annotation for diagram Itinerary details Transmission

Security policies

Security policies represent patterns that shall/ shall not be satisfied against secure business process models inTravel Agency Service. In the following, security policies specified in Travel Agency Service project are reported with the explanation of all the elements included.

Security Policy: "AvailabilityDelegationSR"

AvailabilityDelegationSR is a pattern, i.e. it has to be satisfied in all secure business processes.

The security policy was generated from "availability(Flight Ticket booked, 90%)" security requirement.

Figure 22 show the "AvailabilityDelegationSR" security policy.

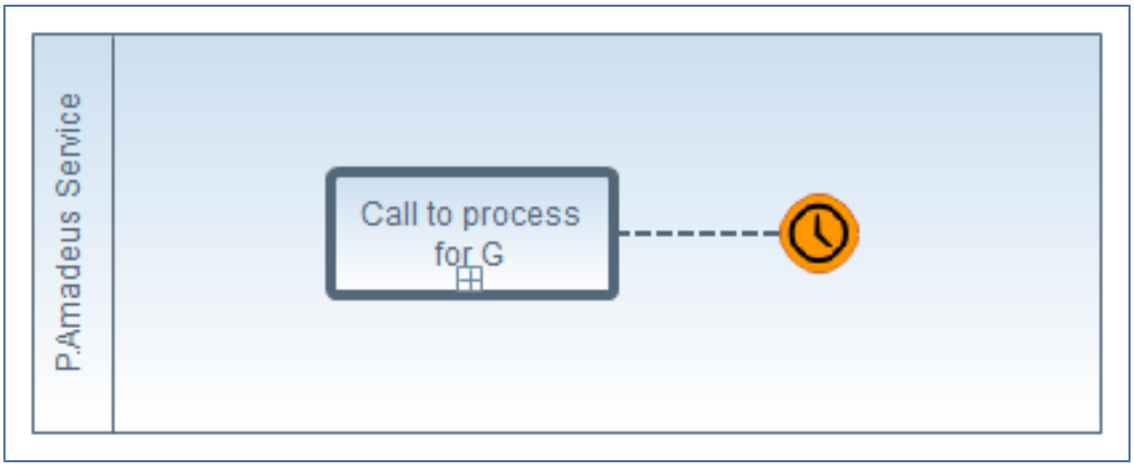

Figure 22 - "AvailabilityDelegationSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.Amadeus Service	Participant		

Table 116 - Participants for diagram "AvailabilityDelegationSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Call to process for G	Flight Ticket booked Process	

Table 117 - Call activities for diagram "AvailabilityDelegationSR"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Availability

We defined the security aspect represented by this security annotation as the ability of a system to ensure that all system's components are available and operational when they are required by authorized users.

Table 118 enlists the availability security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Call to process for G	Enforced by		
	Level	0.0	
	Authorized end users		

Table 118 - "Availability security annotation for diagram AvailabilityDelegationSR

Security Policy: "AvailabilityTransmissionSR"

AvailabilityTransmissionSR is a pattern, i.e. it has to be satisfied in all secure business processes.

The security policy was generated from "availability(Itinerary details, 90%)" security requirement.

Figure 23 show the "AvailabilityTransmissionSR" security policy.

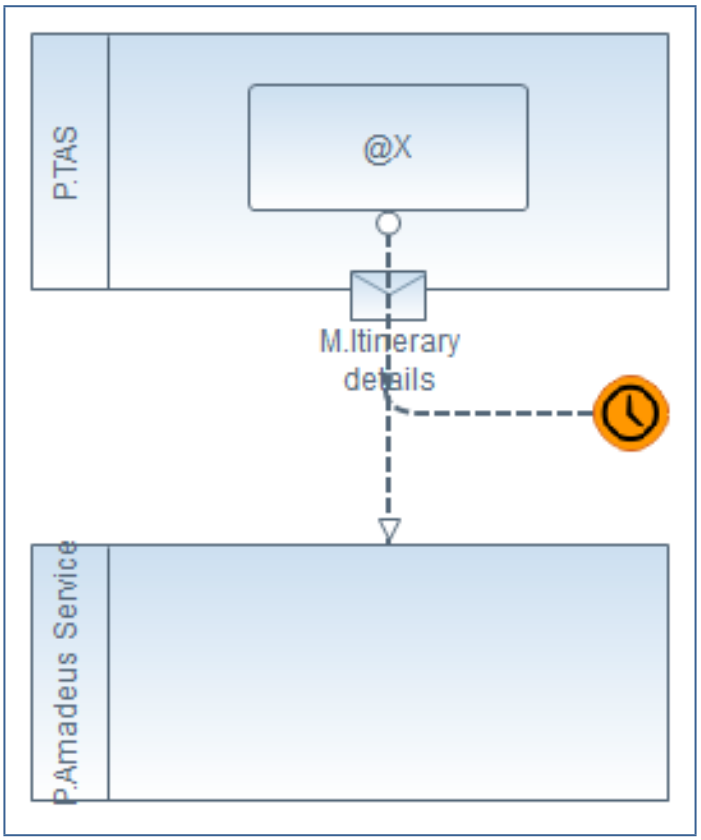

Figure 23 - "AvailabilityTransmissionSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.TAS	Participant		
P.Amadeus Service	Participant		

Table 119 - Participants for diagram "AvailabilityTransmissionSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
@X	Task	

Table 120 - Tasks for diagram "AvailabilityTransmissionSR"

Messages transmissions

Message transmissions represent the communication of messages through message flows between participants.Messages can be used in more than one message transmission, we, therefore, specify all the messages of "AvailabilityTransmissionSR" diagram in Table 121 and the all the message flows of "AvailabilityTransmissionSR" diagram in Table Table 122.

Messages

Messages are the content of the flow of information between two participants.

Name	Description
M.Itinerary details	

Table 121 - Messages for diagram "AvailabilityTransmissionSR"

Message flows

Message flows represent the communication channel between two SecBPMN2 elements.

Message Name	Source	Destination	Description
M.Itinerary details	@X	P.Amadeus Service	

Table 123 - "AvailabilityTransmissionSR" message flows

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Availability

We defined the security aspect represented by this security annotation as the ability of a system to ensure that all system's components are available and operational when they are required by authorized users.

Table 124 enlists the availability security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Message Flow from "@X" to "P.Amadeus Service"	Enforced by		
	Level	0.0	
	Authorized end users		

Table 124 - "Availability security annotation for diagram AvailabilityTransmissionSR

Security Policy: "IntegrityReceiverSR"

IntegrityReceiverSR is a pattern, i.e. it has to be satisfied in all secure business processes.

The security policy was generated from "receiver-integrity(transmitted(TAS,Amadeus Service,Itinerary details))" security requirement.

Figure 24 show the "IntegrityReceiverSR" security policy.

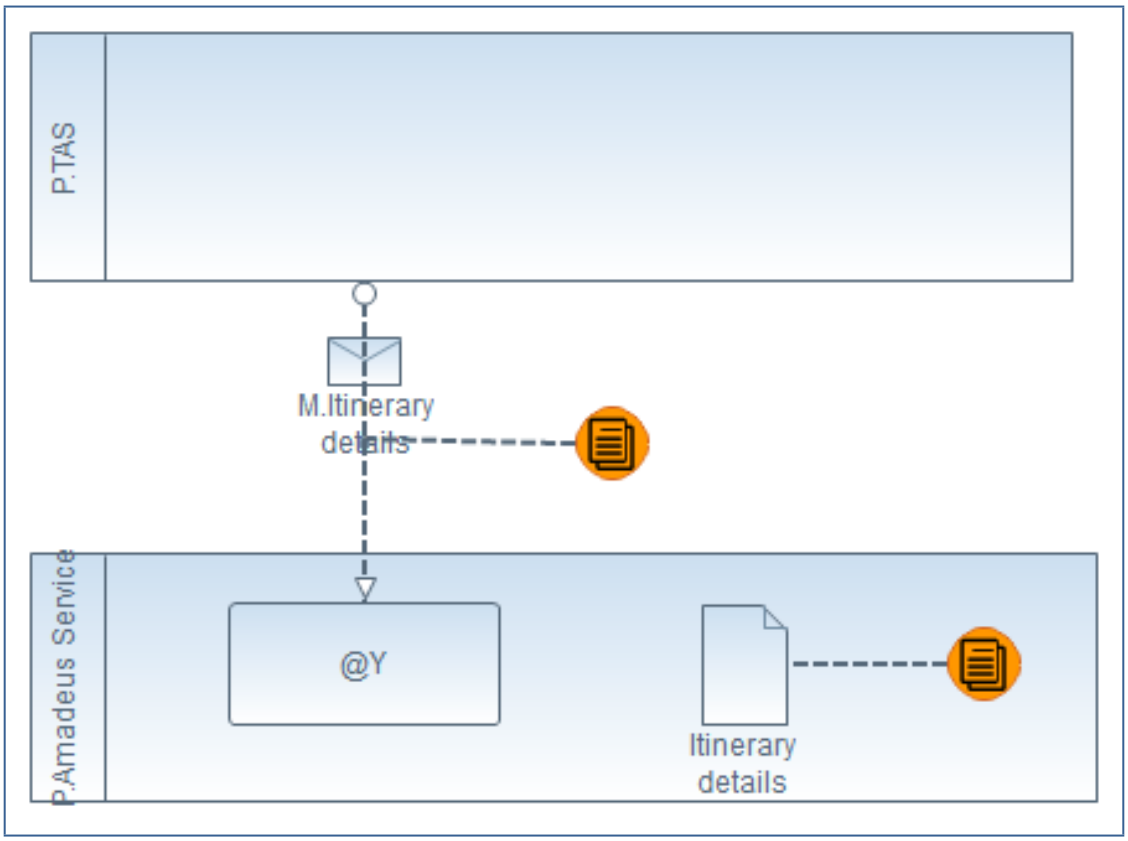

Figure 24 - "IntegrityReceiverSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.TAS	Participant		
P.Amadeus Service	Participant		

Table 125 - Participants for diagram "IntegrityReceiverSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
@Y	Task	

Table 126 - Tasks for diagram "IntegrityReceiverSR"

Data Elements

Data elements represent data in the managed by the business process, i.e. required for their execution or produced by their execution.

Name	Type	Description
Itinerary details	Data Object	

Table 127 - Data elements for diagram "IntegrityReceiverSR"

Messages transmissions

Message transmissions represent the communication of messages through message flows between participants.Messages can be used in more than one message transmission, we, therefore, specify all the messages of "IntegrityReceiverSR" diagram in Table 128 and the all the message flows of "IntegrityReceiverSR" diagram in Table Table 129.

Messages

Messages are the content of the flow of information between two participants.

Name	Description
M.Itinerary details	

Table 128 - Messages for diagram "IntegrityReceiverSR"

Message flows

Message flows represent the communication channel between two SecBPMN2 elements.

Message Name	Source	Destination	Description
M.Itinerary details	P.TAS	@Y	

Table 130 - "IntegrityReceiverSR" message flows

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Integrity

We defined the security aspect represented by this security annotation as the ability of a system to ensure completeness, accuracy and absence of unauthorized modifications in all its components.

Table 131 enlists the integrity security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Message Flow from "P.TAS" to "@Y"	Enforced by		
	Personnel	False	
	Hardware	False	
	Software	False	
Itinerary details	Enforced by		
	Personnel	False	
	Hardware	False	
	Software	False	

Table 131 - "Integrity security annotation for diagram IntegrityReceiverSR

Security Policy: "NoDelegationSR"

NoDelegationSR is a pattern, i.e. it has to be satisfied in all secure business processes.

The security policy was generated from "no-delegation(Flight Ticket booked))" security requirement.

Figure 25 show the "NoDelegationSR" security policy.

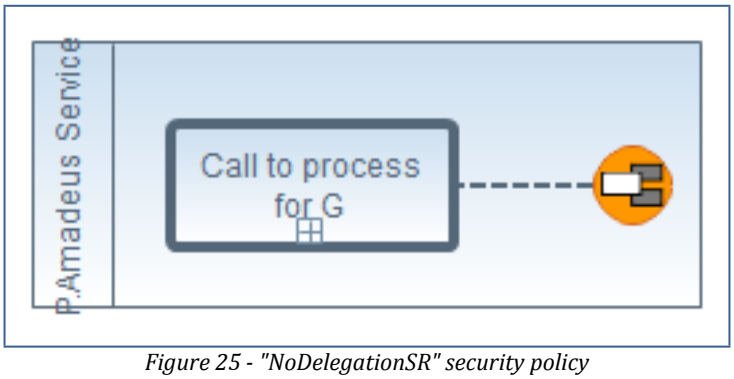

Figure 25 - "NoDelegationSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.Amadeus Service	Participant		

Table 132 - Participants for diagram "NoDelegationSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Call to process for G	Flight Ticket booked Process	

Table 133 - Call activities for diagram "NoDelegationSR"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Non-delegation

We defined the security aspect represented by this security annotation as the ability of the system to require that a set of actions is executed only by the users assigned.

Table 134 enlists the non-delegation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Call to process for G	Enforced by		

Table 134 - "Non-delegation security annotation for diagram NoDelegationSR

Security Policy: "NoDelegationSR"

NoDelegationSR is a pattern, i.e. it has to be satisfied in all secure business processes.

The security policy was generated from "no-delegation(Hotel booked))" security requirement.

Figure 26 show the "NoDelegationSR" security policy.

Figure 26 - "NoDelegationSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.Hotel	Participant		

Table 135 - Participants for diagram "NoDelegationSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Call to process for G	Hotel Process	

Table 136 - Call activities for diagram "NoDelegationSR"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Non-delegation

We defined the security aspect represented by this security annotation as the ability of the system to require that a set of actions is executed only by the users assigned.

Table 137 enlists the non-delegation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Call to process for G	Enforced by		

Table 137 - "Non-delegation security annotation for diagram NoDelegationSR

Security Policy: "NonDisclosureSR"

NonDisclosureSR is an anti-pattern, i.e. no secure business process shall satisfy the security policy.

The security policy was generated from "non-disclosure({Personal data, Itenerary})" security requirement.

Figure 27 show the "NonDisclosureSR" security policy.

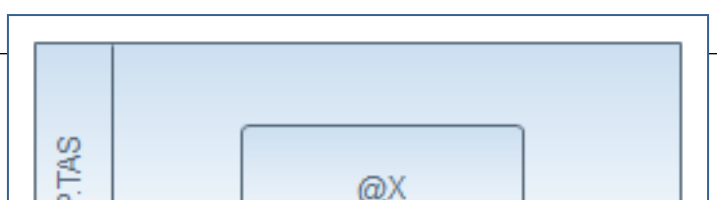

Figure 27 - "NonDisclosureSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.TAS	Participant		
@Z	Participant		

Table 138 - Participants for diagram "NonDisclosureSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
@X	Task	
@Y	Task	

Table 139 - Tasks for diagram "NonDisclosureSR"

Messages transmissions

Message transmissions represent the communication of messages through message flows between participants.Messages can be used in more than one message transmission, we, therefore, specify all the messages of "NonDisclosureSR" diagram in Table 140 and the all the message flows of "NonDisclosureSR" diagram in Table Table 141.

Messages

Messages are the content of the flow of information between two participants.

Name	Description
M.Itinerary details	

Table 140 - Messages for diagram "NonDisclosureSR"

Message flows

Message flows represent the communication channel between two SecBPMN2 elements.

Message Name	Source	Destination	Description
M.Itinerary details	@X	@Y	

Table 142 - "NonDisclosureSR" message flows

Security Policy: "NonModificationSR"

NonModificationSR is an anti-pattern, i.e. no secure business process shall satisfy the security policy.

The security policy was generated from "non-modification({Personal data})" security requirement.

Figure 28 show the "NonModificationSR" security policy.

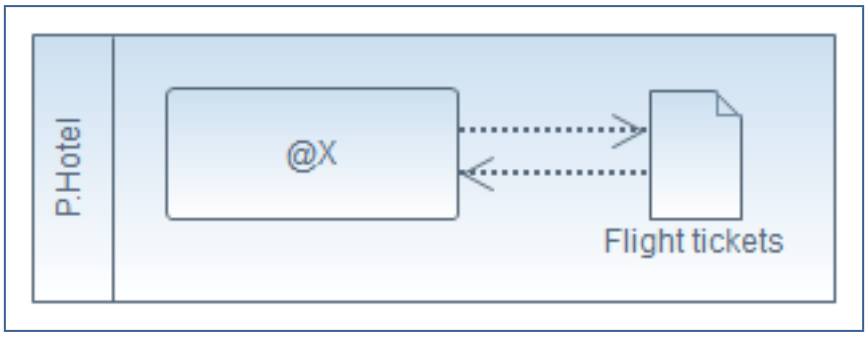

Figure 28 - "NonModificationSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.Hotel	Participant		

Table 143 - Participants for diagram "NonModificationSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
@X	Task	

Table 144 - Tasks for diagram "NonModificationSR"

Data Elements

Data elements represent data in the managed by the business process, i.e. required for their execution or produced by their execution.

Name	Type	Description
Flight tickets	Data Object	

Table 145 - Data elements for diagram "NonModificationSR"

Security Policy: "NonProductionSR"

NonProductionSR is an anti-pattern, i.e. no secure business process shall satisfy the security policy.

The security policy was generated from "non-production({Personal data, Itenerary})" security requirement.

Figure 29 show the "NonProductionSR" security policy.

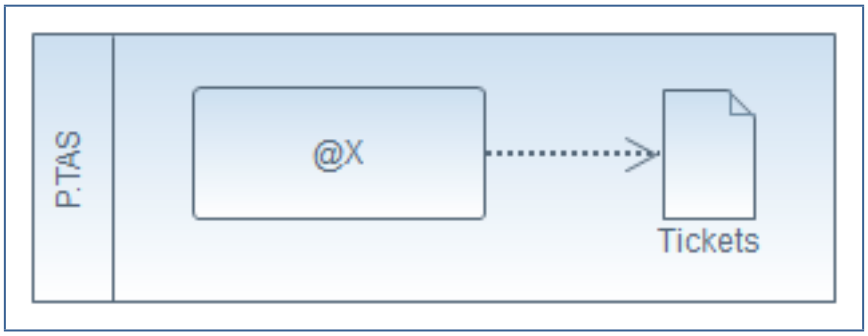

Figure 29 - "NonProductionSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.TAS	Participant		

Table 146 - Participants for diagram "NonProductionSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
@X	Task	

Table 147 - Tasks for diagram "NonProductionSR"

Data Elements

Data elements represent data in the managed by the business process, i.e. required for their execution or produced by their execution.

Name	Type	Description
Tickets	Data Object	

Table 148 - Data elements for diagram "NonProductionSR"

Security Policy: "NonProductionSR"

NonProductionSR is an anti-pattern, i.e. no secure business process shall satisfy the security policy.

The security policy was generated from "non-production({Personal data, Itenerary})" security requirement.

Figure 30 show the "NonProductionSR" security policy.

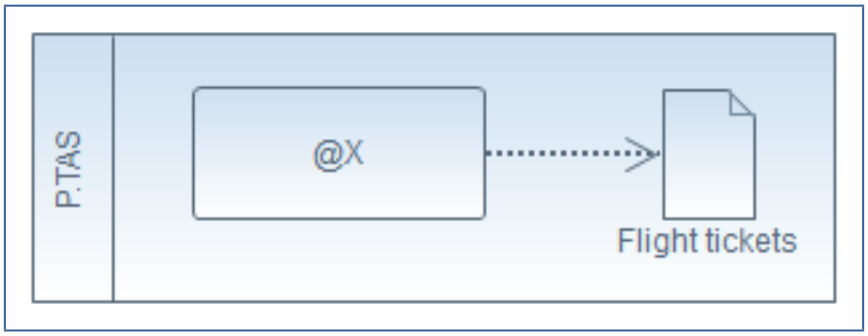

Figure 30 - "NonProductionSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.TAS	Participant		

Table 149 - Participants for diagram "NonProductionSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
@X	Task	

Table 150 - Tasks for diagram "NonProductionSR"

Data Elements

Data elements represent data in the managed by the business process, i.e. required for their execution or produced by their execution.

Name	Type	Description
Flight tickets	Data Object	

Table 151 - Data elements for diagram "NonProductionSR"

Security Policy: "NonProductionSR"

NonProductionSR is an anti-pattern, i.e. no secure business process shall satisfy the security policy.

The security policy was generated from "non-production({Personal data, Itenerary})" security requirement.

Figure 31 show the "NonProductionSR" security policy.

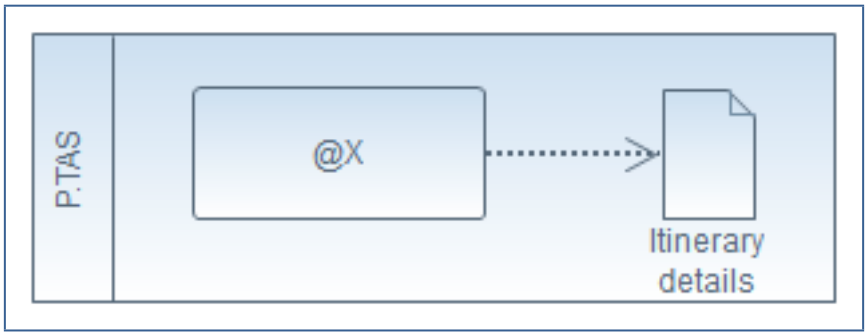

Figure 31 - "NonProductionSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.TAS	Participant		

Table 152 - Participants for diagram "NonProductionSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Tasks

Tasks are activities that represent atomic actions executed in the business processes. Their type characterizes the type of action (Business rule, Choreography, Receive, Send, Script) or the performer (User, Manual, Service).

Name	Type	Description
@X	Task	

Table 153 - Tasks for diagram "NonProductionSR"

Data Elements

Data elements represent data in the managed by the business process, i.e. required for their execution or produced by their execution.

Name	Type	Description
Itinerary details	Data Object	

Table 154 - Data elements for diagram "NonProductionSR"

Security Policy: "NonRepudiationOfAcceptanceSR"

NonRepudiationOfAcceptanceSR is a pattern, i.e. it has to be satisfied in all secure business processes.

The security policy was generated from "non-repudiation-of-acceptance(delegated(TAS,Amadeus Service,Flight Ticket booked))" security requirement.

Figure 32 show the "NonRepudiationOfAcceptanceSR" security policy.

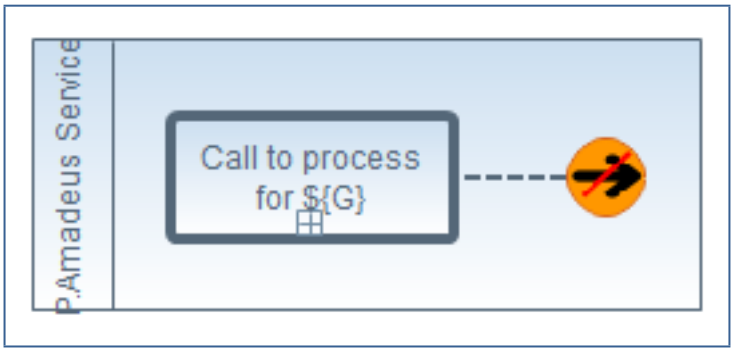

Figure 32 - "NonRepudiationOfAcceptanceSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.Amadeus Service	Participant		

Table 155 - Participants for diagram "NonRepudiationOfAcceptanceSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Call to process for ${G}	Flight Ticket booked Process	

Table 156 - Call activities for diagram "NonRepudiationOfAcceptanceSR"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Non-repudiation

We defined the security aspect represented by this security annotation as the ability of a system to prove (with legal validity) occurrence/non-occurrence of an event or participation/non-participation of a party in an event.

Table 157 enlists the non-repudiation security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Call to process for ${G}	Enforced by		
	Execution	Not Specified	

Table 157 - "Non-repudiation security annotation for diagram NonRepudiationOfAcceptanceSR

Security Policy: "TrustworthinessSR"

TrustworthinessSR is a pattern, i.e. it has to be satisfied in all secure business processes.

The security policy was generated from "trustworthiness(Hotel, delegated(Tourist,Hotel,Hotel booked))" security requirement.

Figure 33 show the "TrustworthinessSR" security policy.

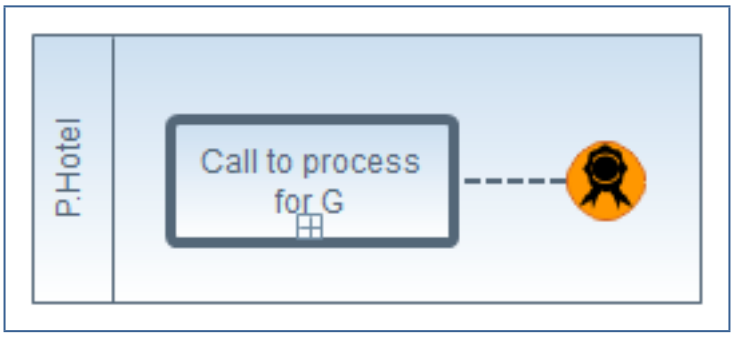

Figure 33 - "TrustworthinessSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.Hotel	Participant		

Table 158 - Participants for diagram "TrustworthinessSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Call to process for G	Hotel Process	

Table 159 - Call activities for diagram "TrustworthinessSR"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Authenticity

We defined the security aspect represented by this security annotation as the ability of a system to verify identity and establish trust in a third party and in information it provides.

Table 160 enlists the authenticity security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Call to process for G	Enforced by		
	Identification	False	
	Authentication	False	
	Trust value	0.0	

Table 160 - "Authenticity security annotation for diagram TrustworthinessSR

Security Policy: "TrustworthinessSR"

TrustworthinessSR is a pattern, i.e. it has to be satisfied in all secure business processes.

The security policy was generated from "trustworthiness(Payment Service, delegated(Hotel Service,Payment Service,Prepayment made))" security requirement.

Figure 34 show the "TrustworthinessSR" security policy.

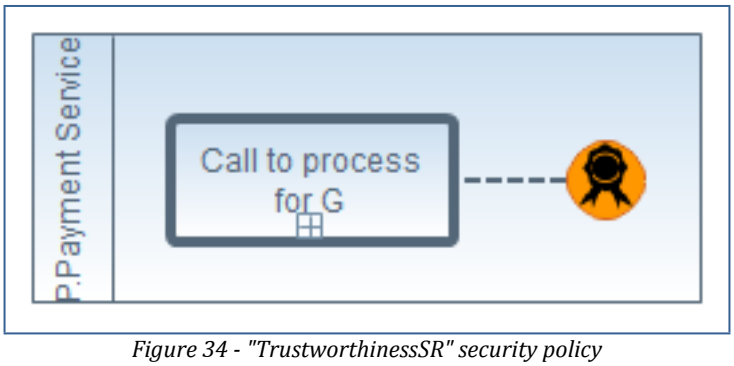

Figure 34 - "TrustworthinessSR" security policy

Participants

Participants are the executor of the business processes.

Name	Type	Contained in	Description
@AnyActor	Participant		
P.Payment Service	Participant		

Table 161 - Participants for diagram "TrustworthinessSR"

Activities

Activities are the main concepts of secure business process: they represent actions executed.

Call Activities

Call activities are activities that represent a call to an external process or a global task. Whenever a call activity is executed, (i) the execution of the business process where the call activity is executed is interrupted; (ii) the business process or global task, referred by the call activity, is executed; (iii) once the referred element finish its execution, the former business process continues its execution.

Name	Referenced element	Description
Call to process for G	Prepayment made Process	

Table 162 - Call activities for diagram "TrustworthinessSR"

Security annotations

Security annotations are annotations that represent security aspects. They can be associated to one or two elements, depending on the type of security annotation. For each security annotation two or more security properties can be specified.

Authenticity

We defined the security aspect represented by this security annotation as the ability of a system to verify identity and establish trust in a third party and in information it provides.

Table 163 enlists the authenticity security annotations specified in project "Travel Agency Service".

Element associated	Property type	Property value	Description
Call to process for G	Enforced by		
	Identification	False	
	Authentication	False	
	Trust value	0.0	

Table 163 - "Authenticity security annotation for diagram TrustworthinessSR

Security policies enforcement analysis

Security enforcement analysis is used to verify if security policies are satisfied against secure business processes. A security policy can be classified as a pattern or as an anti-pattern. In the former case the verification consists in checking if the security policy is satisfied by all business project contained in Travel Agency Service. In the latter case the verification consists in checking if the security policy is NOT satisfied in all business process.

The Security Policies Analysis analysis for Travel Agency Service project didn't find any errors.

Appendix A

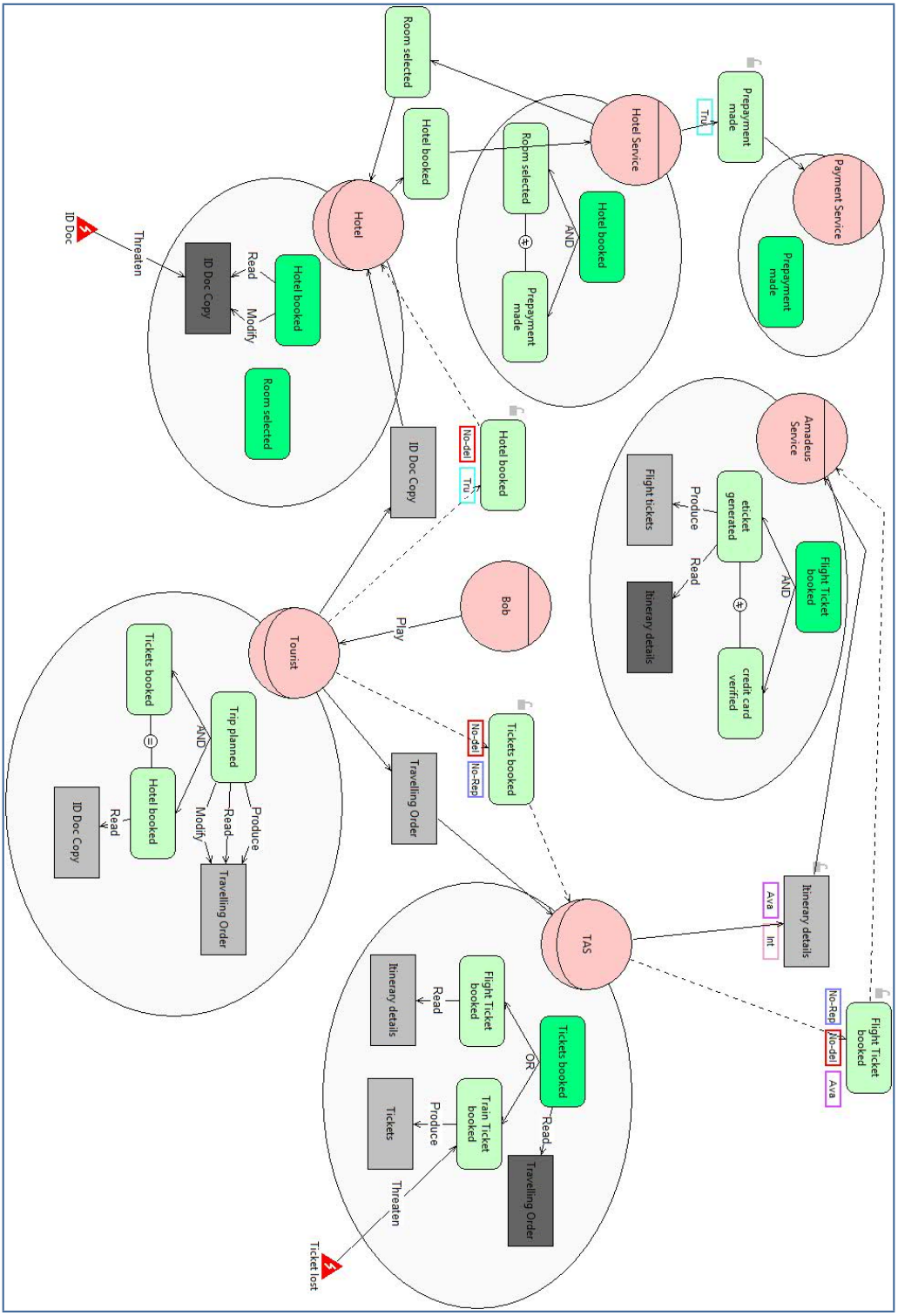

Figure 1 - Social View for the Travel Agency Service project

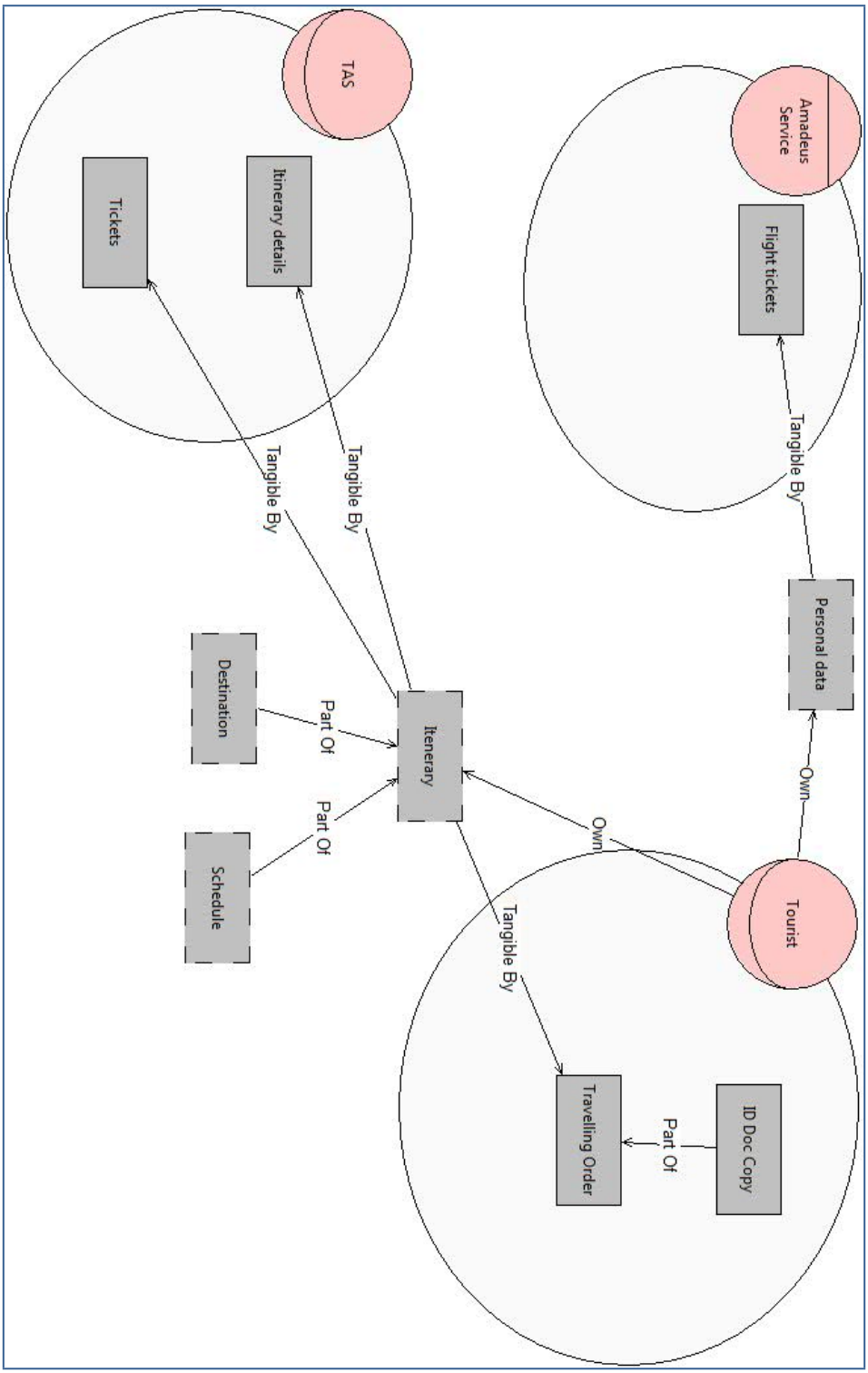

Figure 2 - Information View for the Travel Agency Service project

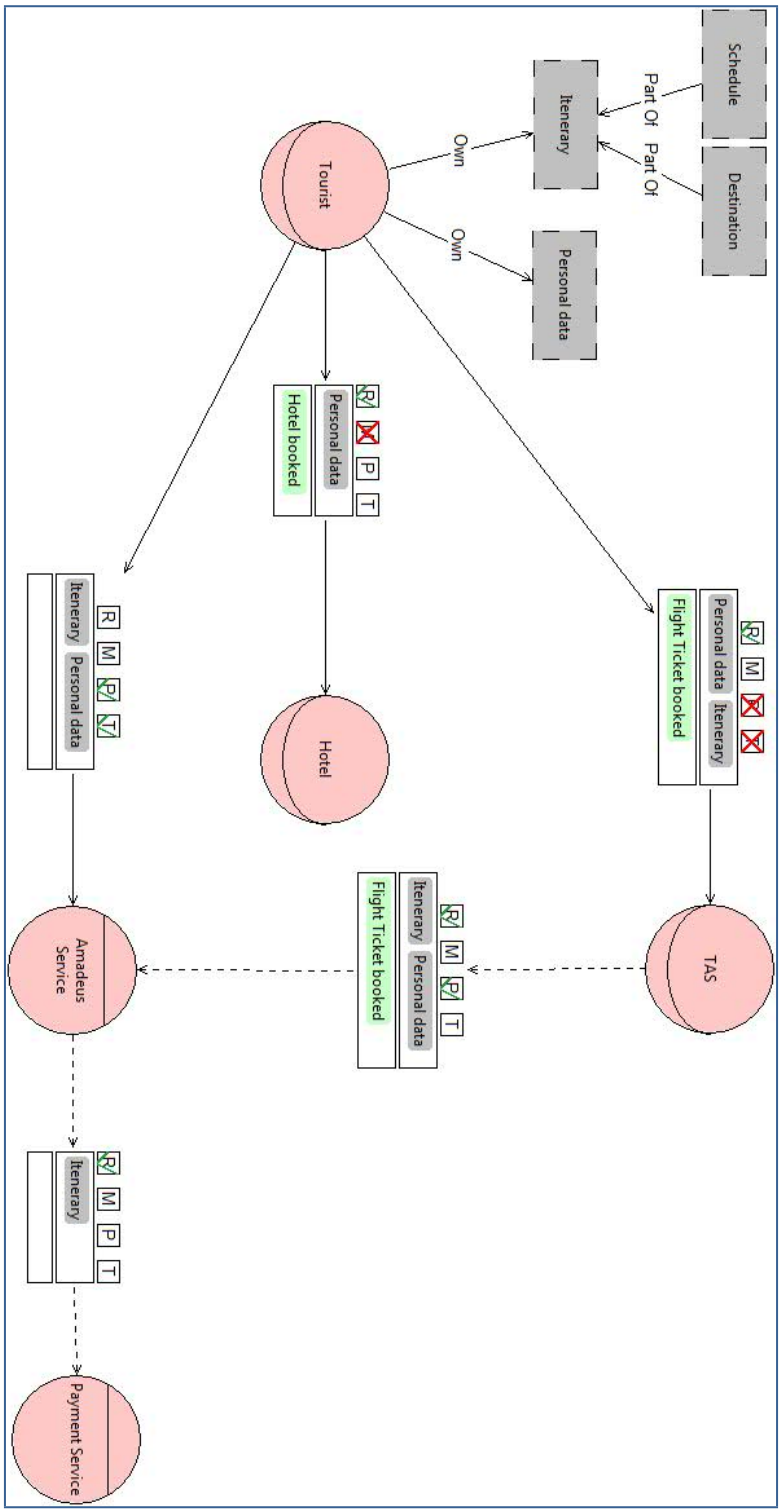

Figure 3 - Authorization View for the Travel Agency Service project

Appendix B

Details of Well-formedness analysis:

- **Empty Diagram**

This check verifies whether the given diagram is empty or not. If that is the case, then no other well-formedness checks are performed. If the diagram is not empty, the well-formedness analysis returns: “No errors found” and continues performing the rest of the well-formedness checks.

- **Goal Single Decomposition**

This check verifies the consistency of goal decompositions. Following the semantics of STS-ml a given goal is decomposed in two or more subgoals. As a result, the decomposition should specify at least two subgoals. Therefore, goal single decomposition verifies whether there are cases of decompositions to a single subgoal.

- **Delegation Child Cycle**

This check verifies the consistency of goal delegations, so that no cycles or loops are identified as a result of the delegatee decomposing the delegatum (delegated goal) and re-delegating back one of the subgoals. Delegation child cycle verifies exactly this and gives a warning in case of inconsistency.

- **Delegated Goal Part Of a Decomposition**

This check verifies that all goals (in the delegatee’s scope) that have been delegated are not child (subgoals) in the decomposition.

- **Inconsistent Contribution Cycle**

This check verifies whether there are loops of positive or negative contribution relationships, and whether this loop contains contradictory relationships. If such a loop is identified, the well-formedness analysis returns a warning.

- **Negative Contributions Between AND Subgoals**

This check verifies that there are no negative contribution relationships between and-subgoals of a given goal (within an actor’s scope). It returns a warning if such a case is identified.

- **Documents PartOf Cycle**

This check verifies whether there is a loop or cycle of Part Of relationships starting from and ending to a given document. If a case like this is verified, a warning is returned enumerating the documents that form the cycle.

- **Informations PartOf Cycle**

This check verifies whether there is a loop or cycle of Part Of relationships starting from and ending to a given document. If a case like this is verified, a warning is returned enumerating the documents that form the cycle.

- **Information No Ownership**

This check verifies that all information have an owner. If there are cases of information without any ownership relationships from any actor in the diagram, the well-formedness analysis returns a warning.

- **Authorizations Validity**

This check verifies that all authorization relationship between two given actors are valid. An authorization relationship specifies authorizations or permissions an actor grants to another on some information, to perform some allowed operations. The authorizations could be limited to a goal scope and they can be re-delegated or not. However, the first two attributes should be specified for an authorization relationship to be valid. If there are no information specified, the well-formedness analysis returns an error. The same applies to the cases, in which no allowed operations are specified.

- **Duplicate Authorizations**

This check verifies that there are no duplicate authorization relationships, that could be merged. There are several cases that are addressed by this check: (i) we encounter two identical authorization, i.e., between the same roles, in the same direction, for the same set of information, allowed operations and goals, and having the same value of transferability; (ii) identify authorization relationships between the same roles, in the same direction, in which one grants permissions that are subset of the other authorization's relationship.

Appendix C

Details of security analysis:

- **No_Delegation Violation check**

This violation is verified whenever a delegatee actor further delegates a goal, over the delegation of which a no-delegation security need is specified from the delegator actor. No-delegation is specified over a goal delegation by the delegator, who requires the delegatee not to further delegate the delegated goal. Therefore, to check for any violations of no-delegation, the analysis searches for redelegations of the delegatum (delegated goal) or any of its subgoals.

- **Redundancy Violation check**

This check verifies if redundancy is satisfied by controlling that single actor redundancy or multi actor redundancy are not violated. At design time we cannot make the distinction between fallback and true redundancy, so they cannot be verified at this stage.Therefore, both fallback redundancy single and true redundancy single are mapped to single actor redundancy. Similarly for multi actor redundancy. The analysis verifies a redundancy violation if one of the following occurs: (1) actor does not decompose the delegated goal in any or-subgoals, for which both types of redundancy are violated (2) actor decomposes the goal into or-subgoals and delegates one to another actor when single actor redundancy has been specified, for which this type of redundancy is violated (3) actor decomposes the goal into or-subgoals, but does not delegate any of the subgoals to another actor when multi actor redundancy has been specified, for which this type of redundancy is violated.

- **Authorization Conflict check**

This task identifies a conflict of authorization whenever at least two authorization relationships for the same information are drawn towards the same actor from two illegible actors (being the owner of information or another authorised actor) such that: (1) one limits the authorization to a goal scope (requiring a need-to-know security need) and the other does not (authorising the actor without any limitations) (2) for the same goals or intersecting goal scopes, different permissions are granted in terms of operations or authority to transfer authoristaion. That is, one passes the actor the authority to perform operations (use, modify, produce, distribute) on a given information, and the other does not (requiring non-usage, non-modification, non-production, non-disclosure); one passes the actor the authority to further transfer authorizations and the other requires no further authorizations take place.

- **Non_Reading Violation**

This violation is detected whenever an actor discloses information without having the right to distribute it. Non-disclosure expresses the need of not disclosing or further distributing the given information to other actors, apart from the authoriser. Thus, authority to distribute the information is not passed. The way actors exchange information is through document provision. In order to disclose some information, an actor would have to provide to others the document(s) containing that information. Hence, to verify if there are any unauthorized disclosures of information, the analysis checks for provisions of documents representing the given information from any unauthorized actors towards other actors.

- **Non_Modification Violation**

This violation is detected whenever an actor modifies information without having the right to modify it. Non-modification expresses the need that information should not be changed (modified), i.e. authority to modify the information is not granted. To verify if there could be any violations of non-modification, the analysis looks if the authorisee (or an actor that is not authorised by authorised party) modifies the given information. For this, it searches for modify relationships from any goal of this actor to any document representing the given information.

- **Non_Production Violation**

This violation is detected whenever an actor produces information without having the right to produce it. Non-production expresses the need that information should not be produced in any form, i.e. authority to produce the information is not granted. To verify if there could be any violations of non-production, the analysis checks whether if the authorisee (or an actor that is not authorised by authorised party) produces the given information. For this, it searches for produce relationships from any goal of this actor to any document representing the given information.

- **Non_Disclosure Violation**

This violation is detected whenever an actor discloses information without having the right to distribute it. Non-disclosure expresses the need of not disclosing or further distributing the given information to other actors, apart from the authoriser. Thus, authority to distribute the information is not passed. The way actors exchange information is through document provision. In order to disclose some information, an actor would have to provide to others the document(s) containing that information. Hence, to verify if there are any unauthorized disclosures of information, the analysis checks for provisions of documents representing the given information from any unauthorized actors towards other actors.

- **NTK Violation**

This violation is detected whenever an actor uses, modifies or produces information for other purposes (goal achievement) than the ones for which it is authorized. Need-to-know requires that the information is used, modified, or produced in the scope of the goals specified in the authorization. This security need concerns confidential information, which should not be utilised for any other purposes other than the intended ones. To verify if there could be any violations of need-to-know, security analysis checks if the authorisee (or an actor that is not authorised by any authorised party) uses, modifies or produces the given information while achieving some goal different from the one it is authorised for. In a nutshell, it searches for need, modify, or produce relationships starting from goals different from the specified ones towards documents representing the given information.

- **Explicit non-reauthorization**

Verifies whether a given actor transfer rights to others even when it does not have the authority to further delegate rights.

- **Non-reauthorization Violation: read**

Verifies whether a given actors transfer to other actors the right to use a given information, without having itself the right to do so.

- **Non-reauthorization Violation: modify**

Verifies whether a given actors transfer to other actors the right to modify a given information, without having itself the right to do so.

- **Non-reauthorization Violation: produce**

Verifies whether a given actors transfer to other actors the right to modify a given information, without having itself the right to do so.

- **Non-reauthorization Violation: transmit**

Verifies whether a given actors transfer to other actors the right to distribute a given information, without having itself the right to do so.

- **Sod Goal Violation**

This violation is detected whenever a single actor may perform both goals, between which an SoD constraint is expressed. Goal-based SoD requires that there is no actor performing both goals among which SoD is specified. To perform this verification, the analysis checks that the final performer of the given goals is not the same actor.

- **Bod Goal Violation**

This violation is detected whenever a single actor may perform both goals, between which an SoD constraint is expressed. Goal-based SoD requires that there is no actor performing both goals among which SoD is specified. To perform this verification, the analysis checks that the final performer of the given goals is not the same actor.

- **Agent Play Sod**

This check verifies the consistency of the Separation of Duty (SoD) constraint between roles. This constraint requires that two roles are not played by the same agent, therefore the check verifies whether there is one agent playing both roles. If that is the case an error is identified, otherwise the check finds no errors.

- **Agent Not Play Bod**

This check verifies the consistency of the Binding of Duty (BoD) constraint between roles. This constraint requires that two roles are played by the same agent, therefore the check verifies whether there is one agent playing both roles. If that is the case the check finds no errors, otherwise an error is identified.

- **Organizational Constraint Consistency**

This check verifies that no conflicting organisational constraints (SoD or BoD) between goals are specified.

Appendix D

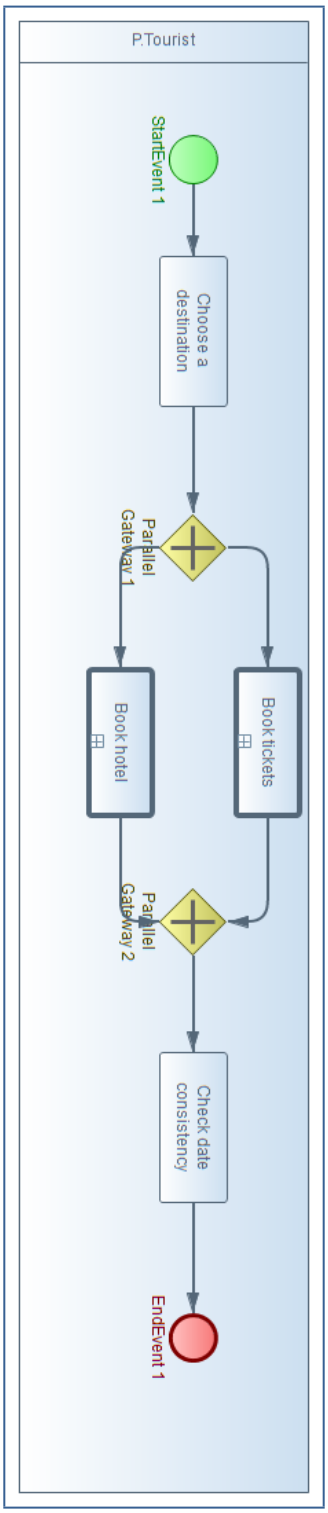

Figure 4 - "Trip planned Process" Diagram

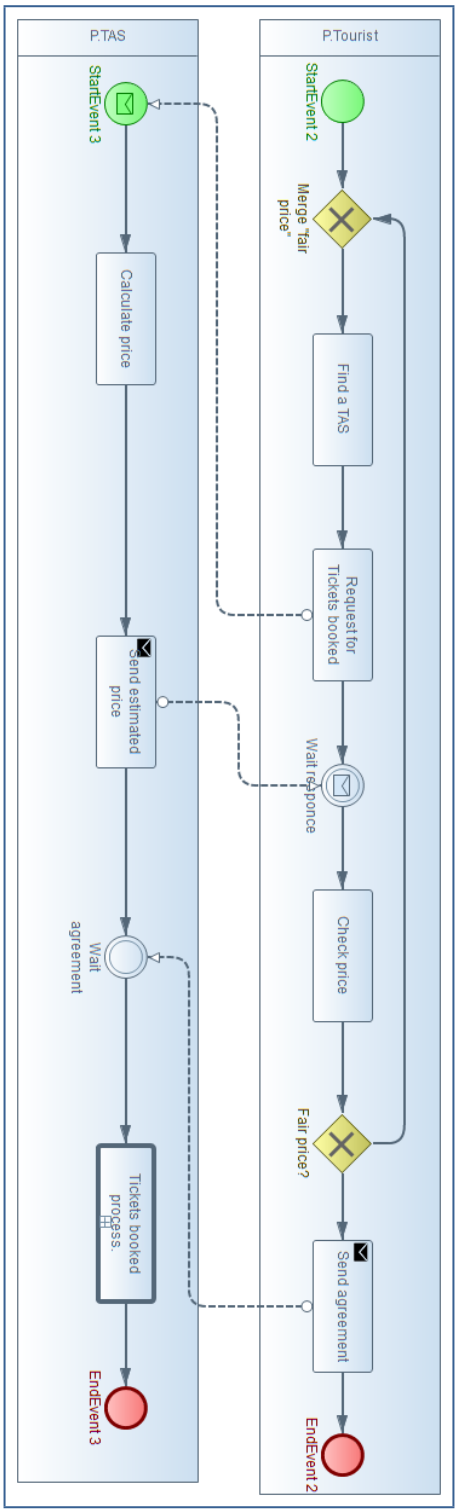

Figure 6 - "Tickets booked delegation" Diagram

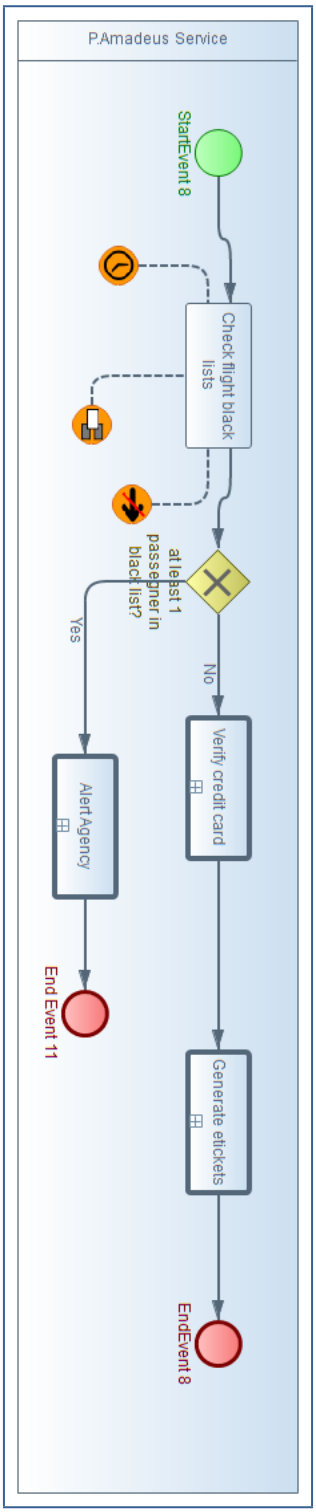

Figure 10 - "Flight Ticket booked Process" Diagram

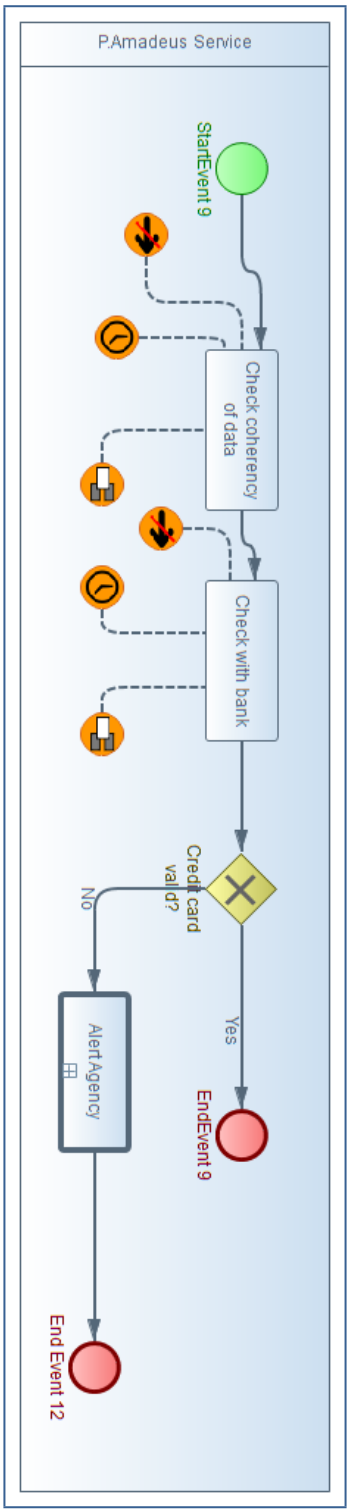

Figure 11 - "credit card verified Process" Diagram

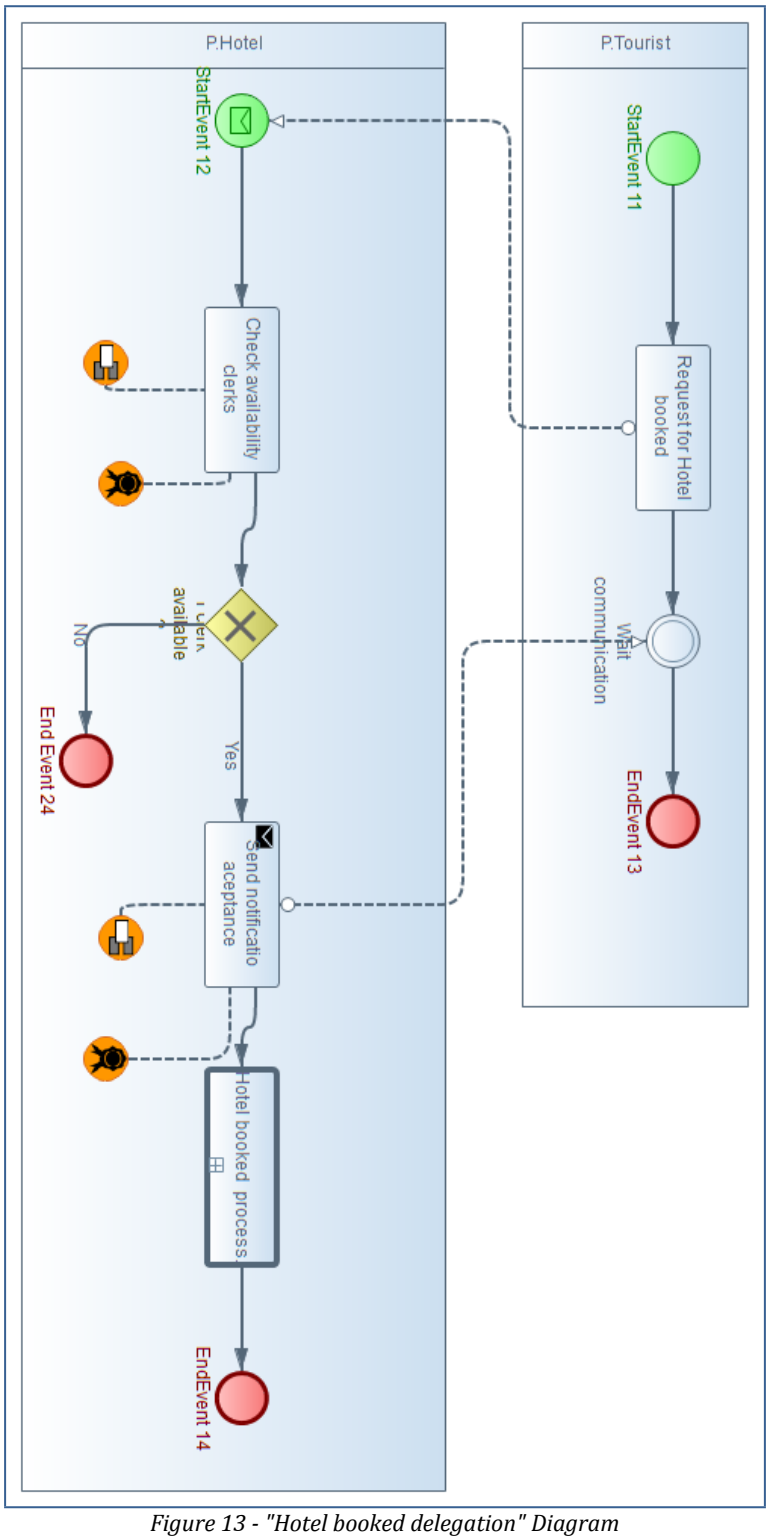

Figure 13 - "Hotel booked delegation" Diagram

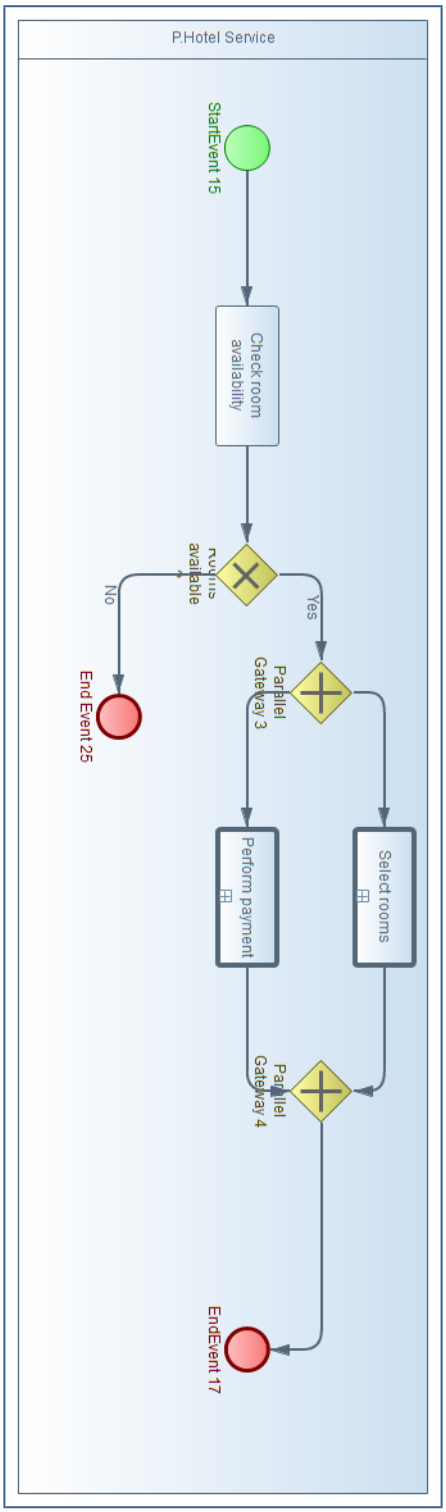

Figure 15 - "Hotel booked Process" Diagram

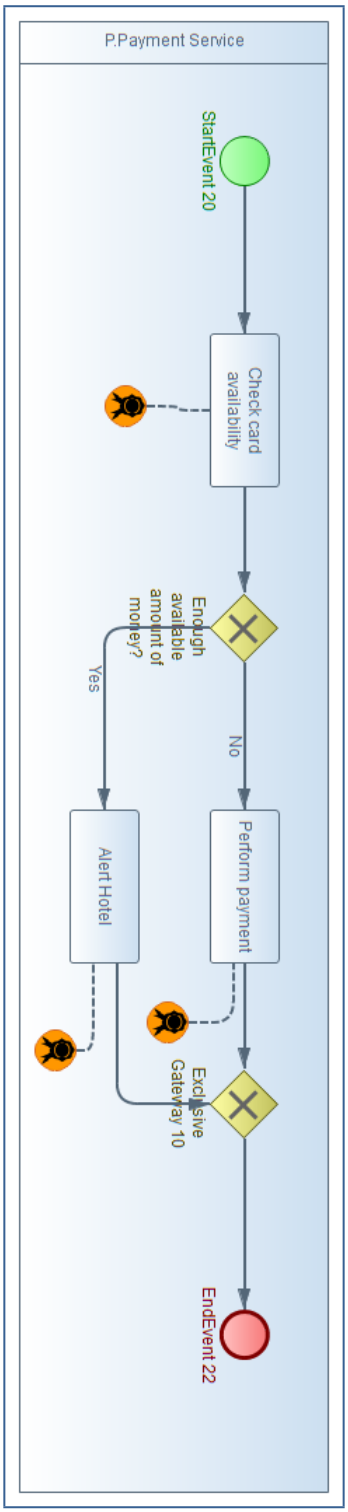

Figure 18 - "Prepayment made Process" Diagram